2010-12

Countering small boat terrorism in territorial sea

Singh, Jaswinder.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COUNTERING SMALL BOAT TERRORISM IN TERRITORIAL SEA

by

Jaswinder Singh

December 2010

Thesis Advisor:	Alex Bordetsky
Second Reader:	Michael Jaye

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2010	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE Countering Small Boat Terrorism in Territorial Sea	5. FUNDING NUMBERS
6. AUTHOR(S) Captain Jaswinder Singh, Indian Navy	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense, U.S. Government, Indian Navy or the Government of India. IRB Protocol Number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Terrorists exploit surprise in successful attacks; security forces are generally unaware of the source of these attacks. In today's information age, terror threats may originate with transnational organizations or exploit the territory of failed, weak or neutral states. Countering maritime terrorism by eliminating terrorists on land is the best solution; however, it may not be feasible, and if feasible could require many years. This thesis utilizes Game Theory to analyze various counterterrorism strategies, and infers how security forces could tilt the game of small boat terror attacks to their advantage. Since Israel has immense experience in countering small boat terrorism, Israeli coastal defense is analyzed, examining how detection and identification enhance Maritime Space Transparency (MST), adapting Maritime Domain Awareness (MDA) to territorial sea. Since MST needs to be maintained continuously in time and large spatial domains, the feasibility of utilizing Automatic Identification System (AIS), Inverse Synthetic Aperture Radar (ISAR) and electro-optical sensors on aerostats, and AIS and Synthetic Aperture Radar (SAR) from Low Earth Orbit (LEO) satellites to generate a Common Operating Picture (COP) is explored. The optimum number of aerostats fitted with an appropriate sensor suite is calculated with multi-criteria optimization to provide more than 89% MST. The thesis concludes with recommendations, such as amending existing International Maritime Organization AIS fitment policy from size-based to role-based fitment.

14. SUBJECT TERMS Countering Small Boat Terrorism, Game Theory, Maritime Domain Awareness (MDA), Maritime Space Transparency (MST), Automatic Identification System (AIS), Aerostat, Low Earth Orbit (LEO) Satellite, Synthetic Aperture Radar (SAR), Inverse Synthetic Aperture Radar (ISAR), Common Operating Picture (COP), Multi Criteria Optimization (MCO).	15. NUMBER OF PAGES 101
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COUNTERING SMALL BOAT TERRORISM IN TERRITORIAL SEA

Jaswinder Singh
Captain, Indian Navy
B.S., Indore University, 1987
M.S., Madras University, 2004

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS
(INFORMATION OPERATIONS)

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Jaswinder Singh

Approved by: Dr. Alex Bordetsky
Thesis Advisor

Dr. Michael Jaye
Second Reader

Dr. Gordon H. McCormick
Chairman, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Terrorists exploit surprise in successful attacks; security forces are generally unaware of the source of these attacks. In today's information age, terror threats may originate with transnational organizations or exploit the territory of failed, weak or neutral states.

Countering maritime terrorism by eliminating terrorists on land is the best solution; however, it may not be feasible, and if feasible could require many years. This thesis utilizes Game Theory to analyze various counterterrorism strategies, and infers how security forces could tilt the game of small boat terror attacks to their advantage.

Since Israel has immense experience in countering small boat terrorism, Israeli coastal defense is analyzed, examining how detection and identification enhance Maritime Space Transparency (MST), adapting Maritime Domain Awareness (MDA) to territorial sea.

Since MST needs to be maintained continuously in time and large spatial domains, the feasibility of utilizing Automatic Identification System (AIS), Inverse Synthetic Aperture Radar (ISAR) and electro-optical sensors on aerostats, and AIS and Synthetic Aperture Radar (SAR) from Low Earth Orbit (LEO) satellites to generate a Common Operating Picture (COP) is explored.

The optimum number of aerostats fitted with an appropriate sensor suite is calculated with multi-criteria optimization to provide more than 89% MST. The thesis concludes with recommendations, such as amending existing International Maritime Organization AIS fitment policy from size-based to role-based fitment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Automatic Identification System
COP	Common Operating Picture
CV	Conditional Variable
DV	Dependent Variable
ECDIS	Electronic Chart Display and Information System
ETA	Estimated Time of Arrival
IV	Independent Variable
LEO	Low Earth Orbit
LTTE	Liberation Tigers of Tamil Eelam
MDA	Maritime Domain Awareness
MPA	Maritime Patrol Aircraft
MST	Maritime Space Transparency
SAR	Synthetic Aperture Radar
SOTDMA	Self Organized Time Division Multiple Access
TDMA	Time Division Multiple Access
UAV	Unmanned Aerial Vehicles
USV	Unmanned Surface Vehicles
VHF	Very High Frequency
VTS	Vessel Traffic System

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

At the outset, I would like to thank my advisors, Dr. Alex Bordetsky and Dr. Michael Jaye, for their outstanding knowledge and advice for completing this thesis. Guidance provided by Dr. Alex Bordetsky with his excellent domain knowledge has been instrumental in directing my research towards low earth orbit satellites and introducing me to multi-criteria optimization. Dr. Michael Jaye's continuous and timely analytical support with exceptional feedback made this research possible. To both my advisors, much credit is due, and I thank them both for their patience and brilliant guidance.

There are many others, I wish to thank for their contributions and support in making this thesis possible; the conceptual contributions of Dr. Gordon H McCormick and Dr. Frank R. Giordano towards this thesis have been exceptional. Dr. Gordon H McCormick's rationale of information asymmetry between insurgents and state forms the backdrop of this thesis with similar asymmetry being exploited by the terrorists in today's information age. Dr. Frank R. Giordano sparked my interest in Game Theory, which forms the backbone of this thesis and analytically guided the research towards an appropriate direction for completing the loop.

I would also like to thank Robin Longshaw for her patience in editing this thesis.

I also take this opportunity to thank my wife, Manju, and our two daughters, Simran and Sameera, for their patience and regular support, which allowed me to complete this thesis within the allotted time.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. IDENTIFICATION OF THE PROBLEM

The 2008 terrorist attack in Mumbai, India's financial capital, drew widespread condemnation across the world. The attack killed more than 173 people and wounded 308, and "for 62 hours, from the night of 26 November to the morning of 29 November, the city of Mumbai was held hostage to terror attacks."[1] Since 1993, Mumbai has witnessed many coordinated bomb explosions by terrorists; but the attack on 26 November 2008, wherein the attackers utilized the sea to infiltrate the country, was the first of its kind in India.

Figure 1. TAJ HOTEL IN MUMBAI UNDER ATTACK

[1] Namrata Goswami, "IDSA Comment - Mumbai Attacks: A Deadly Performance," Institute of Defense Studies and Analysis, December 05, 2008, http://www.idsa.in/idsastrategiccomments/MumbaiAttacks_NGoswami_051208 (accessed January 26, 2010).

"It has now come to light from the interrogation of the arrested terrorist, Mohammad Ajmal Amir Iman, a resident of Faridkot village in Pakistan's Punjab province, that 10 Lashkar-e-Toiba (LeT) men left Karachi harbor and rowed out to the Arabian Sea in the early morning of 23 November and later on hijacked a Porbandar-based fishing boat Kuber to reach Mumbai."[2] The infiltrators then split into smaller groups and attacked different locations in Mumbai, including hotels, railway stations, pubs and residential areas. Prior to these terror attacks, there had been many incidents of small boat terror attacks carried out worldwide by the Palestinians, LTTE and Al-Qaeda; but none of these incidents, though serious by themselves, caused mass casualties or destruction on the level of the Mumbai attacks.

Countries like Israel and Sri Lanka have been combating these types of small boat terror attacks in their territorial sea for many years; historically, Israel has been the longest victim of such attacks.

> Historically, Israel's main experience with maritime terrorism came in the 1970s. When, for the first time Palestinian terror organizations gained experience with and developed maritime terrorism tactics that are still relevant today. Three out of the four major terrorist attacks in Israel in the 1970s were maritime infiltration attacks.[3]

Although Israel has been a victim of small boat terrorism since 1970, the most devastating of these types of terror attacks prior to the Mumbai attacks, were those undertaken by Al-Qaeda against warships and merchantmen.

> Al-Qaeda's most notable success in deploying terror technique was its devastating attack on the USS Cole (DDG 67) in Aden on October 12, 2000. The attack killed 17 sailors and injured 39 others, leaving the vessel with a 40 by 60 foot hole in its port side; repairs to the vessel cost nearly $250 million. Two years later, on October 6, 2002, Al-Qaeda bombers in a small boat filled with

---

2 Namrata Goswami, "IDSA Comment - Mumbai Attacks: A Deadly Performance."

3. Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel," International Institute for Counterterrorism. September 24, 2007, http://www.ict.org.il/Articles/tabid/66/Articlsid/251/currentpage/6/Default.aspx (accessed February 14, 2010).

> explosives rammed the French tanker Limburg at Mukalla, as it was approaching the Ash Shihr Terminal off the Yemeni coast. This attack killed one crewmember and spilled 90,000 barrels of oil from the vessel's 397,000-barrel cargo.[4]

These small boat terror attacks by Al Qaeda, were in clear emulation of the tactics developed by the LTTE, which involved ramming a boat laden with explosives into selected maritime targets. It is apparent that in the recent past, terrorist organizations like Al Qaeda have very successfully adapted the proven attack methods of LTTE, on a couple of incidents against the U.S. and its allies.

In today's information age, the terrorists' transnational network enables them to share the operational tactics of contemporary, proven attack methods, and also encourages other terrorist organizations to adopt such methods. Thus, the possibility of small boat terror attacks, similar to the 2008 Mumbai terror attacks, in the future and against other countries, especially those combating terrorism, cannot be ignored.

B. PURPOSE AND SCOPE

Countering maritime terrorism by eliminating terrorists on land is unquestionably the best solution; however, this may not always be feasible and if feasible could require many years. The purpose of this thesis, therefore, is to suggest an implementable solution to counter the threat of small boat terrorism in territorial sea by utilizing existing theories and technologies, even if the efforts on land have not effectively countered the terrorist base camps. The scope of the thesis has been restricted to the territorial sea, as it is only in these waters that a state exercises sovereign jurisdiction. This is in accordance with the United Nations Convention on the Law of the Sea, which states, "the sovereignty of a

[4] John C. K. Daly, "Terrorism and Piracy: The Dual Threat to Maritime Shipping," *Global Terrorism Analysis,* August 15, 2008, http://www.jamestown.org/programs/gta/Terrorism and Piracy The Dual Threat to Maritime Shipping - The Jamestown Foundation.mht (accessed February 07, 2010).

coastal state extends, beyond its land territory and internal waters, and in the case of an archipelagic state, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea."[5]

C. RESEARCH QUESTION

Terrorists exploit surprise to ensure the success of a terror attack. Target security forces are generally unaware of the terror attacks' "who, where and when;" leading to the question: can small boat terror attacks in territorial sea be effectively countered? The surprise factor ensures information advantage to the terrorists for negating the force advantage of unsuspecting security forces. Therefore, to successfully counter small boat terrorism in territorial sea, security forces have to overcome terrorists' information asymmetric advantage.

D. HYPOTHESES

Navies worldwide have utilized and are utilizing Maritime Domain Awareness (MDA), which is all about collecting and amalgamating information from various sources into a Common Operating Picture (COP), for generating actionable intelligence. MDA could, therefore, be adapted for the territorial sea, reducing information asymmetry between terrorists and maritime security forces. This would also provide necessary transparency in the desired maritime space, to interdict small boats heading for terror attacks in these waters. Certain analysts do not agree with this hypothesis and articulate alternative hypotheses some of which call for pre-emptive or retaliatory strikes against terrorist base camps.

---

5 "United Nations Convention on the Law of the Sea - Part II," *United Nations web sites,* http://www.un.org/Depts/los/convention_agreements/texts/unclos/part2.htm (accessed March 01, 2010).

E. LITERATURE REVIEW

1. Conceptual Literature

The existing theories on counterterrorism have been organized into two categories of offensive and protective philosophies. These have been tabulated below:

Offensive	Protective
1. Pre-emptive strikes: - U.S. National Strategy for combating terrorism 2003.[6]	1. Enhancing MDA to mitigate maritime threats: - Views of Dana Goward, Director of Assessment, Integration, and Risk Management U.S. Coast Guard in 2009.[7] - U.S. DHS' Strategy and Plans 2009 to Counter Small Vessel Threats.[8]
2. Retaliatory strikes: - Israeli counter maritime terrorism strategy in the 1970s.[9]	2. Deterring terrorism: - It can be done, by Robert F Trager and Dessislava P. Zagorcheva.[10]

Table 1. OFFENSIVE AND PROTECTIVE PHILOSOPHIES

6 *U.S. National Strategy for Combating Terrorism,* https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

7 Dana Goward, "Maritime Domain Awareness -- The Whole is Greater than the Sum of its," *U.S. Coast Guard,* April 20, 2009, http://www.uscg.mil/comdt/blog/2009/04/maritime-domain-awareness-whole-is.asp (accessed March 02, 2010).

8 "DHS' Strategy and Plans to Counter Small Vessel," *Department of Homeland Security Office of Inspector General,* September 2009, http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-100_Sep09.pdf (accessed March 02, 2010).

9 Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

10 Robert F. Trager and Dessislava P Zagorcheva, "Deterring Terrorism: It Can be Done," *International Security 3, no. 3*, Winter 2005/06, 87.

2. Empirical Literature

The preliminary literature review is enunciated under the following heads:

- Israel – Israeli coastal defense has been identified as a case study to identify the procedures and technologies utilized in territorial sea, to enhance their MDA. The review of historical data is also envisaged to validate the importance of enhancing MDA. Some of the literature, which has been identified on this subject is:
  - The Threat of Maritime Terrorism to Israel.[11]
  - Israeli coastal defense.[12]
  - Policy on Automatic Identification System by ships and boats off Israeli coast.[13]
- Maritime Domain Awareness (MDA) – Preliminary review of the literature on MDA primarily indicates that although efforts by various countries such as the U.S., Australia and India, are underway to detect and identify small boats, but no substantial gain(s) has/have been made in identifying small boats. The literature in this field comprises:
  - U.S. National plan to achieve Maritime Domain Awareness for the national strategy for maritime security.[14]
  - U.S. Coast Guard Nationwide Automatic Identification System.[15]

---

[11] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

[12] Ibid.

[13] *State of Isarel Ministry of Transport and Road Safety,* June 18, 2009, http://en.mot.gov.il/index.php?option=com_content&view=article&id=145:rad17m&catid=17:noticetomariners&Itemid=12 (accessed June 30, 2010).

[14] "U.S. National Plan to achieve Maritime Domain Awareness," October 2005, http://www.virginia.edu/colp/pdf/NSMS-National-Plan-to-Achieve-Maritime-Domain-Awareness.pdf (accessed March 02, 2010).

- U.S. Boat Association Reproaches Small Boat Tracking Proposals, by Mike Godfrey.[16]

- Automatic Identification System (AIS) – The literature reviewed on the AIS reveals, that while this system was primarily designed for the navigation safety of vessels at sea, but it is being utilized by some countries such as Australia, Canada and many European countries, for building up their MDA. This system has promise towards identification, therefore its fitment on small boats for their identification and Low Earth Orbit (LEO) for covering more area, is being presently deliberated world over. The literature identified under this subject, comprises:

  - International Maritime Organization's policy regarding fitment of AIS.[17]

  - Efficacy of fitting AIS on small boats.[18]

  - Spaced-based AIS.[19]

- Promising technologies – It is envisaged to review existing technologies, which presently are not being utilized in the maritime domain, but which could promise the much-needed enhanced MDA in the territorial sea for countering the threat of small boat terrorism.

---

15 *U.S. Nationwide Automatic Identification System (NAIS),* http://www.uscg.mil/ACQUISITION/nais/ (accessed March 02, 2010).

16 Mike Godfrey, *U.S. Boat Association Reproaches Small Boat Tracking Proposals,* December 16, 2009, http://www.tax-news.com/asp/story/story_marine.asp?storyname=40704 (accessed March 02, 2010).

17 *IMO adopts comprehensive maritime security measures,* December 13, 2002, http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689 (accessed January 22, 2010).

18 Dziewicki, Marek. *The Role of AIS for Small Ships.* Department of ATON Technique and Radionavigation Systems Report, Gdynia: BalticMaster Gdynia, February 2007.

19 Høye K. Gudrun, Eriksen Torkild, Meland J. Bente and Narheim T. Bjørn, *Space based AIS for Global Maritime Traffic Monitoring,* Norway: Norwegian Defence Research Establishment, 2007.

The following existing and promising technologies have been identified:

- Tethered Aerostat Sensor Suite:
  - Potential Military Use of Airships and Aerostats – CRS report for Congress.[20]
  - The U.S.'s RAID program: Small Systems, Big Surveillance Time.[21]
- Low Earth Orbit (LEO) satellites for monitoring of AIS.[22]
- Synthetic Aperture Radar (SAR) fitted LEO satellites.[23]

F. FRAMEWORK AND METHODOLOGY

Although the suicide attacks against USS Cole and MV Limburg were cases of small boat terrorism, the attacks were not carried out in the territorial sea of the countries whose Flag these ships were flying. Israel has been fighting maritime terrorism, especially small boat terrorism, in its territorial sea since 1953, and today it has the best coastal defense in the world.[24] Considering these facts, the thesis was undertaken in three separate and sequential steps, as:

- The various existing theories on counterterrorism were reviewed in the first step, and the most appropriate of them was identified. Utilization of game theory was envisaged to identify the most

---

[20] Christopher Bolkcom, *Potential Military Use of Airships and Aerostat,* CRS Report for Congress, CRS Web, 2005.

[21] "The USA's RAID Program: Small Systems, Big Surveillance Time," *Defense Industry Daily,* July 19, 2009, http://www.defenseindustrydaily.com/the-usas-raid-program-small-aerostats-big-surveillance-time-02779/ (accessed February 07, 2010).

[22] "Satellite-Based AIS: One Giant Leap for Vessel Tracking," *Boats,* June 06, 2010, http://features.boats.com/boat-content/2010/06/satellite-based-ais-one-giant-leap-for-vessel-tracking/ (accessed August 24, 2010).

[23] "RADARSAT-2," *Imaging Notes,* Fall 2008, http://www.imagingnotes.com/go/article_free.php?mp_id=147 (accessed August 24, 2010).

[24] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

appropriate theory to counter small boat terrorism in the territorial sea. This step also identified the independent and dependent variables of the identified theory.

- The second step analyzed a case study appropriate to the identified theory, to study the causal relationship between the independent and dependent variables. This step would also linked the probabilities of occurrence between the various variables and identified the existence of a conditional variable(s), if any.
- Multi-criteria optimization was utilized in the final step to find Pareto optimum solutions.

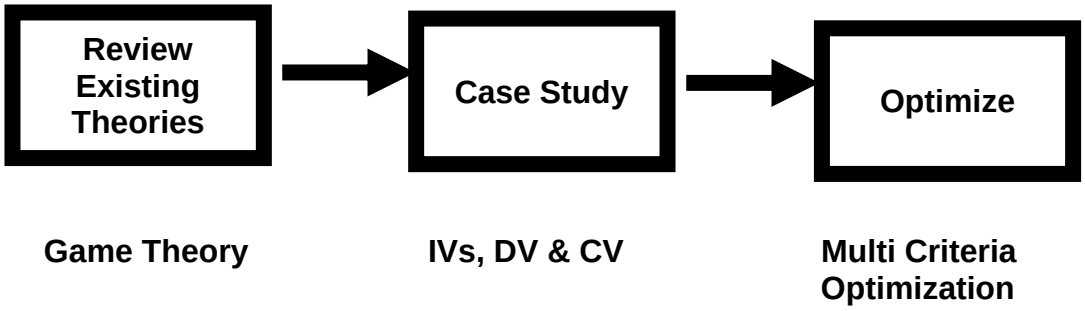

Figure 2. THESIS FLOW CHART

1. Existing Theories

The existing counterterrorism theories after literature review have been categorized under the following heads:

- Offensive philosophy comprising pre-emptive and retaliatory strikes.
- Protective philosophy comprising of deterrence and information symmetry by MDA.

Though there would be more voices attempting to articulate better ways and means to effectively counter terrorism, the majority of them could be classified into the above-mentioned categories, or as a combination of them. The

final outcome of modeling by game theory is very much dependent upon the two specific players, and also the mathematical interval scaling applied (i.e., transforming the payoffs from a scale of 1–4 to 1–10) by utility theory would affect the weighted preferences of the outcome; however, a preliminary application of game theory indicates that reducing information asymmetry between the security forces and terrorists would draw the game in favor of the former. Additionally, detection and identification have been identified as the independent variables and Maritime Space Transparency (MST) as a dependent variable.

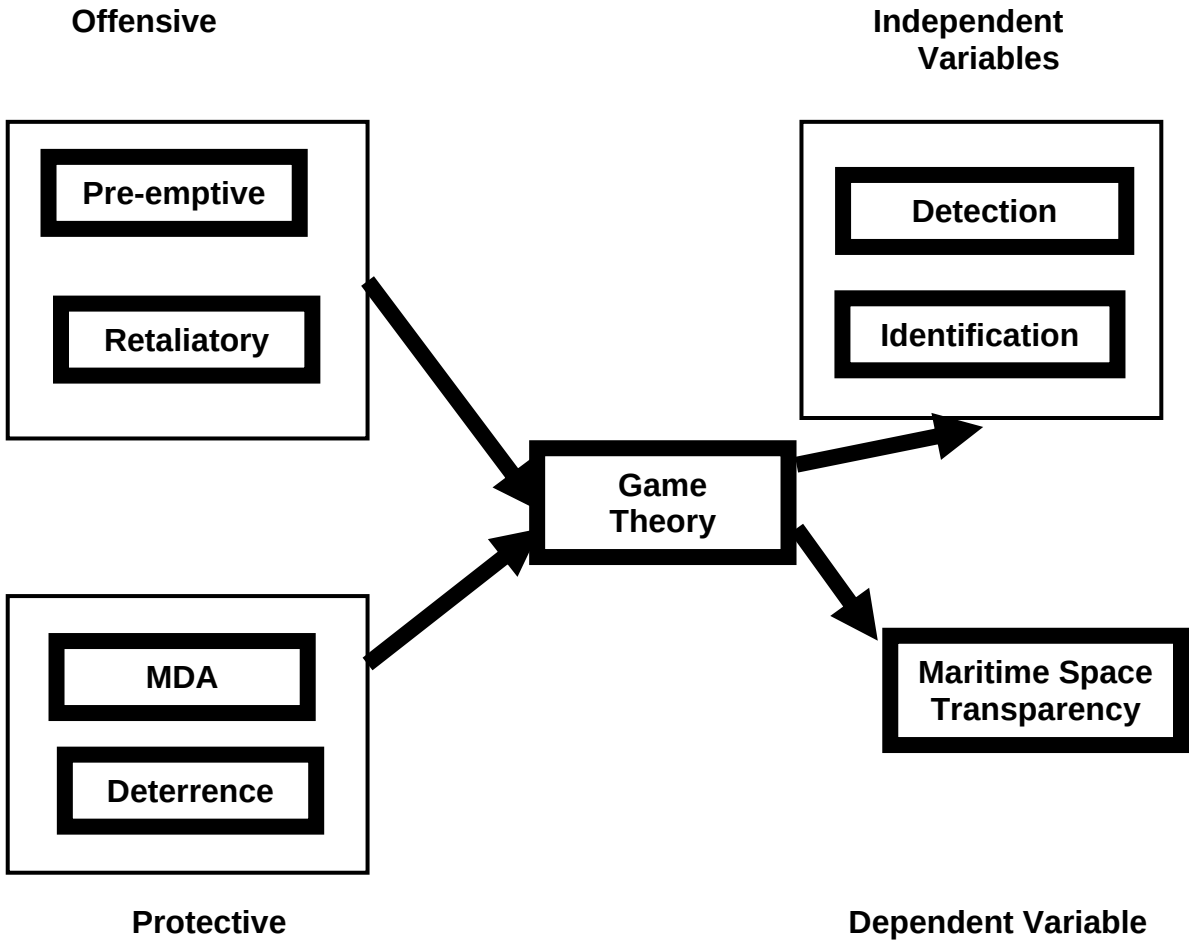

Figure 3. GAME THEORY FLOW CHART

2. Case Study

As mentioned, Israel has been fighting small boat terrorism in its territorial sea for more than five decades and today has the best coastal defense in the world. Therefore, the Israeli coastal defense was selected as a case study to analyze how this country has implemented detection and identification to enhance Maritime Space Transparency in its territorial sea. The technologies (i.e., automated shore radars, shore-based AIS, Maritime Patrol Aircraft (MPA), Unmanned Aerial Vehicles (UAVs), Unmanned Surface Vehicles (USVs), and procedures (i.e., AIS policy) being utilized by Israeli coastal defense were analyzed in order to establish a causal relationship between the independent variables (i.e., detection and identification) and dependent variable (Maritime Space Transparency). Historical data, indicating increase or decrease in small boat terrorism in Israeli territorial sea after the country adapted MDA to its territorial sea, were utilized for testing the recommended hypothesis. Israel's limited coastline of approximately 200 km, a conditional variable (environment) of this case, had to be considered, and others routes to overcome this constraint had to be analyzed to implement the recommended hypothesis.

3. Optimization

Since the asymmetry of information has to address the "when" and "where" in addition to the "who" of terror attacks, continuous monitoring in the time and space domains for detection and identification were required. Israeli coastal defense covers a coastline of approximately 200 km, but for longer coastlines, alternative routes had to be explored. The feasibility of utilizing aerostats and LEO satellites, which could enhance MST to adapt MDA for territorial sea, were also explored. The limitation and restriction of the technologies recommended for adapting MDA to territorial sea were identified, so that these could be utilized to optimize the dependent variable of MST by multi-criteria optimization techniques. Moreover, since MDA is all about amalgamating information from various sources to generate a COP as actionable intelligence, the thesis concludes by recommending a solution that could be attached with the existing MDA in order to adapt it to the territorial sea.

THIS PAGE INTENTIONALLY LEFT BLANK

II. EXISTING COUNTERTERRORISM THEORIES

A. STRATEGY

"All men can see the tactics whereby I conquer, but what none can see is the strategy out of which victory is evolved."[25] As articulated by Sun Tzu, the correct strategy is critical for victory. But one could ask, "What is strategy?" Yarger's strategy model states, "strategy is all about how (way or concept) leadership will use the power (means or resources) available to the state to exercise control over sets of circumstances and geographic locations to achieve objectives (ends) that support state interests."[26] In order to identify the most appropriate philosophy to counter the threat of small boat terror attacks in the territorial sea, the existing counterterrorism theories (how of the strategy) based on the identified problem (objective of strategy), need to be rationally analyzed. Since humans live on land, terror attacks at sea always originate from one country or another. As described by Sri Lankan Navy Commander Vice Admiral Thisra Samarasinghe while addressing the 19th International Sea Power Symposium in Rhode Island, U.S., "A terrorist organization with maritime capability needs to operate from foreign soil or a safe base; the prevention of the use of foreign soil for all illegal activity particularly on remote islands and isolated coastal stretches needs to be addressed."[27] Therefore, other than homegrown terrorism, small boat terror attacks in the territorial sea could either be sponsored by another country or undertaken by a terrorist organization operating from foreign territory. Though it is still debatable, there could be cases of pure

---

25 Sun Tzu, "The Art of War," *Classics Archive,* http://classics.mit.edu/Tzu/artwar.html (accessed April 21, 2010).

26 Harry R. Yarger, "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model," *USAWC Guide to National Security Issues, Vol I: Theory of War and Strategy*, 43–49, Carlisle, United States: Strategic Studies Institute of the U.S. Army War College (SSI), 2008.

27 Vice Admiral Thisra Samarasinghe, "Sri Lankan Navy's role in eradicating international maritime terrorism." *Sri Lanka Guardian.* October 25, 2009. http://www.srilankaguardian.org/2009/10/sri-lankan-navys-role-in-eradicating.html (accessed May 07, 2010).

homegrown terrorism without external assistance; nevertheless, in the case of such homegrown terrorism both offensive and protective counterterrorism can be undertaken, while in the case of the involvement of another state, offensive counterterrorism actions would amount to international armed conflict. In such cases, the success of countering these types of attacks by their sheer nature would greatly depend upon the role played by the nation state from which the terrorist organizations operate.

> Conflict has been a central theme throughout human history and literatures. It arises whenever two or more individuals, with different values, compete to try to control the course of events. Game theory uses mathematical tools to study situation involving both conflict and cooperation. Its study was greatly stimulated by the publication in 1944 of the monumental "Theory of Games and Economic Behavior by John von Neumann and Oskar Morgenstern." The players in a game, who may be people, organizations, or even countries, choose from a list of options available to them – that is, courses of action they might take – that are called strategies. The strategies chosen by the players lead to outcome, which describe the consequences of their choices. We assume that the players have preferences for the outcome: they like some more than others. Game theory analyzes the rational choices of strategies – that is, how players select strategies to obtain preferred outcomes.[28]

The application of Game theory would thus provide appropriate mathematical tools to identify the most appropriate philosophy to counter the small boat terror attacks. To rationally analyze counterterrorism theories with Game theory, existing theories of counterterrorism have been categorized as either offensive or protective.

B. OFFENSIVE PHILOSOPHY

"We will not rest until terrorist groups of global reach have been found, have been stopped, and have been defeated – U.S. President George W. Bush,

[28] Consortium for Mathematics, *For All Practical Purposes: Introduction to Contemporary Mathematics,* New York: W H Freeman & Company, 1996.

06 November 2001."[29] Post-9/11, the then president of United States articulated a very offensive counterterrorism strategy as stated in the 2003 — U.S. national strategy for combating terrorism. This to date has been the most offensive counterterrorism strategy followed by any nation in the world. Historically, Israel has utilized the retaliatory strike strategy against other states and terrorist organizations operating from foreign territory to counter maritime terrorism, as pointed out by Lorenz "the maritime terrorism attacks in the 1970s and early 1980s had direct implications on Israel's defense doctrines, which called for even harder military retaliation against terrorist infrastructures, thereby often invading the sovereign territory of third state."[30] Although, the offensive strategy against terrorists can be further sub-divided into pre-emptive or retaliatory strikes, depending upon the time at which the offensive is launched; but in both the cases action to counterterrorism actions against organizations operating from foreign territory, without the concurrence or cooperation of the host country would amount to an international armed conflict as per the Geneva Conventions' Rules of Law for Armed Conflict, which states that "an armed conflict confined geographically to the territory of a single state can, however, be qualified as international if a foreign state intervenes with its armed forces on the side of the rebels fighting against government forces."[31] An offensive strike against terrorist base camps, especially the planners and executors of small boat terror attacks, could also be deep inside foreign territory and would be very difficult to justify to the international community in today's age where information travels faster than a bullet.

> Following the Coastal Road attack, Israel launched a wide scope of military actions, in order to prevent Palestinian terrorism from Lebanon. On 14 March 1978, Israel launched Operation Litani. During the seven-day offensive, the IDF first captured a belt of land approximately 10 kilometers deep with the aim of pushing

---

29 U.S. National Strategy for Combating Terrorism.

30 Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

31 *Geneva Academy of International Humanitarian Law and Human Rights,* http://www.adh-geneva.ch/RULAC/qualification_of_armed_conflict.php (accessed May 07, 2010).

> Palestinian militant groups, particularly the PLO, away from the border with Israel. The operation was later expanded in order to occupy all the territory, with the exception of Tyre, up to the Litani River. However, despite the superiority of the IDF and the high casualties on both sides, the operation did not destroy the Palestinian terror infrastructure in Lebanon. Israel's invasions into Lebanon also resulted in UN Resolution 425 and Resolution 426 calling for the withdrawal of Israeli forces from Lebanon and the establishment of the UN Interim Force in Lebanon (UNIFIL) with the mandate to restore peace and sovereignty to Lebanon.[32]

Terrorists, akin to insurgents, always exploit the information advantage (i.e., the terrorists identity and location are not precisely known) to counter the force advantage of the counterterror forces. Therefore, even with the cooperation of the host country, counterterror forces first have to locate the terrorists in order to counter them, and this would definitely cause some collateral damage, even if so-called smart intelligent weapons are used. Countering the executors of small boat terror attacks in the planning or training phase is undoubtedly a better counterterrorism strategy considering the earliest and furthest elimination of the enemy; but it could be very expensive in terms of finances and resources (including human), if these operations are stretched in time. According to the U.S. Congressional Research Service Report of 2009, U.S. since 9/11 has spent $944 billion on the war on terror.

> Based on DOD estimates and budget submissions, the cumulative total for funds appropriated from the 9/11 attacks through FY2009, total funding enacted to date for DOD, State/USAID and VA for medical costs for the wars in Iraq, Afghanistan and enhanced security is $944 billion.[33]

C. PROTECTIVE PHILOSOPHY

As articulated by Goward, Director of Assessment, Integration and Risk Management of U.S. Coast Guard in his article "Maritime Domain Awareness -- The Whole is Greater than the Sum of Its:"

---

[32] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

[33] Amy Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11,* CRS Report for Congress, Congressional Research Service, 2009.

> The recent piracy cases off the coast of Somalia have illustrated, there is a significant need for Maritime Domain Awareness - the ability to detect, classify and identify vessels at sea. We need greater awareness on the high seas as well as along our coastlines for safety and security purposes. This need has been universally agreed upon by the international maritime community.[34]

Further, in his view, "maritime threats, including piracy and the potential use of small vessels, can be mitigated through greater MDA."[35] The concept of MDA requires collection of information from various sources including but not limited to the state-of-the-art electronic sensors from different platforms, such as satellites, ships, aircrafts, unmanned aerial vehicles, unmanned surface vehicles and shore-based stations. The information so collated is then amalgamated and transformed, by detecting and identifying vessels at sea, into actionable intelligence in the form of Common Operating Picture (COP). Based on the classification of the contacts in the COP, which comprises friendly, hostile or unclassified contacts, the targets can be further investigated or engaged. "The Navy has achieved MDA for years at the tactical level to dominate areas surrounding Carrier and Expeditionary Strike Groups, but in the context of the global war on terrorism (GWOT), MDA takes on a strategic dimension."[36] Though MDA has been institutionalized recently, this concept has been in existence ever since man ventured onto the seas. In earlier days, mariners utilized optical devices like telescopes and binoculars for building up domain awareness, by sighting and visually identifying objects around their ships. The information so obtained was exchanged amongst the ships of the fleet using various types of flags. As technology advanced, the means accommodated its incorporation, but the concept has remained the same, which necessitates the collation of information for its transformation into actionable intelligence, by detecting and identifying the contacts in the desired domain. Therefore, the same system of

---

[34] Dana Goward, "Maritime Domain Awareness -- The Whole is Greater than the Sum of Its."

[35] Ibid.

[36] "Maritime Domain Awareness," *GlobalSecurity,* http://www.globalsecurity.org/intell/systems/mda.htm (accessed May 07, 2010).

MDA, which has been in existence for years, if adapted to the territorial sea, could counter the threat of small boat terror attacks. There is no doubt that terrorists today are unpredictable, networked and constantly evolving new tactics, compared to the conventional enemy of the yesteryears. An efficient network of sensors to provide MDA in the territorial sea, would therefore ensure protection against the threat of small boat terrorism. As pointed out by Akiva J. Lorenz, in "The Threat of Maritime Terrorism to Israel,"

> The maritime terrorism attacks in the 1970s and early 1980s had direct implications on Israel's defense doctrines, which called for even harder military retaliation against terrorist infrastructures, thereby often invading the sovereign territory of third states. Moreover, these attacks showed the necessity to increase the navy's budget, in order to improve Israel's existing coastal defense layout and establish new regulations relating to maritime safety.[37]

Unlike the situation in the 1980s, where the terror threat could be limited to a terrorist organization; today the terror threat could be simultaneously from many terrorist organizations with similar ideology, could involve transnational terrorist organizations like Al-Qaeda, or could even involve the exploitation of some other states' territory. The present situation is only likely to further complicate as more terrorist organizations exploit the information age to connect on ideology, utilize the Internet for training and secure communication, emulate tactics from past successful terror attacks, and exploit the territory of some failed, weak, rouge or even neutral states. Such an environment has to be considered the background while analyzing the protective philosophy of MDA involving enhanced maritime surveillance for coastal defense and the offensive philosophy of pre-emptive and / or retaliatory strikes against the terrorists' base camps with the game theory.

D. GAME THEORY

In order to analyze the offensive and protective philosophies used to counter the threat of small boat terrorism in territorial sea, it is important to identify the players and various options available to them. As stated earlier, in

[37] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

case of homegrown terrorism, both offensive action on land and protective action at sea can be initiated against the terrorist organizations. But, in case of involvement of another country in terms of state-sponsored terrorism or if terrorist organization are operating from foreign territory, a dilemma whether to take offensive action arises. The two players in this game then happen to be the terror victim state and terror origin state. The options available to the terror origin state are to take action against the terrorists or not to take action against them. The terror victim state could follow either the offensive philosophy, which as pointed out earlier would be construed as an international armed conflict according to the Geneva Conventions' Rules of Law for Armed Conflict; or protective philosophy by adapting MDA for the territorial sea. There could also be more voices attempting to articulate better philosophy with which to handle such terror attacks; but the majority of them could be classified as one of these categories, or as a combination of them. Additionally, as all possible situations need to be analyzed to have a logical outcome by Game Theory, the above two likely responses by terror victim state would be utilized, as these are all encompassing.

1. Game Setup

To progress the game theory, it has been assumed that both players are rational and are attempting to maximize their strategy, and that the terror victim state has the military capability to launch an offensive against the terror origin state.

- Options for terror origin state:
  - (C) - Takes no action against the terrorists (i.e., those involved from their country in small boat terror attacks).
  - (D) - Takes action against the terrorists (i.e., those involved from their country in small boat terror attacks).
- Options for terror victim state:
  - (A) – Offensive.

- (B) – Protective.

		Terror Origin State	
		No Action against Terrorists (C)	Action against Terrorists (D)
Terror Victim State	Offensive (A)	AC	AD
	Protective (B)	BC	BD

Figure 4. GAME SETUP

The four possible outcomes of the game would be:

- AC – Terror origin state takes no action against the terrorists; terror victim state goes offensive.
- AD – Terror origin state takes action against the terrorists: terror victim state goes offensive.
- BC – Terror origin state takes no action against the terrorists; terror victim state remains protective.
- BD – Terror origin state takes action against the terrorists; terror victim state remains protective.

It would be safe to assume that different perspectives could also be justified and could yield different rankings, but for this game the following rank order has been established based on the fact that the cost of armed conflict including human resources would be much higher than establishing an effective MDA in territorial sea,

as according to the U.S. Congressional Research Service Report of 2009, the U.S. since 9/11 have spent $944 billion on the war on terror:[38]

- Terror victim state:
    - 4 – Best – Terror origin state takes action against the terrorists; terror victim state remains protective.
    - 3 – Next Best – Terror origin state takes no action against the terrorists; terror victim state remains protective.
    - 2 – Least Best – Terror origin state takes no action against the terrorists; terror victim state goes offensive.
    - 1 – Worst – Terror origin state takes action against the terrorists: terror victim state goes offensive.

Considering the higher cost of offensive action, the payoff for protective has been rated higher than that of offensive.

- Terror origin state:
    - 4 – Best – Terror origin state takes no action against the terrorists; terror victim state remains protective.
    - 3 – Next Best – Terror origin state takes action against the terrorists; terror victim state remains protective.
    - 2 – Least Best – Terror origin state takes no action against the terrorists; terror victim state goes offensive.
    - 1 – Worst – Terror origin state takes action against the terrorists: terror victim state goes offensive.

Based on the ranking of the various options, the outcome of the game without the players communicating would be as:

[38] Amy Belasco, *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11,* CRS Report for Congress.

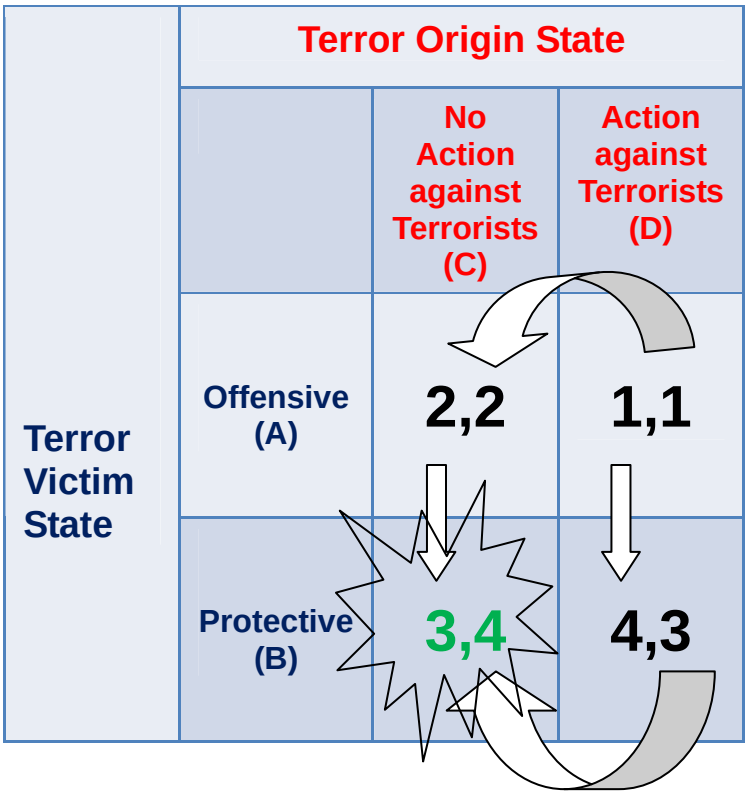

Figure 5. PARTIAL CONFLICT GAME

In Figure 5, the arrows indicate both players maximizing their payoffs. As indicated above, each player has a pure dominant strategy. The terror origin state's pure dominant strategy is not to take any action against the terrorists and the terror victim state's pure dominant strategy is to remain protective. The Nash Equilibrium is a point from which neither player can benefit by unilaterally changing its strategy. The Nash Equilibrium of this game is (BC), (3, 4), i.e., the terror origin state takes no action against the terrorists and the terror victim state continues to remains protective.

2. Strategic Moves

The strategic moves of this game with both players communicating with each other would be:

a. First Move

- Should terror victim state move first:
    - If terror victim state does A, then terror origin state does C, outcome (2, 2).
    - If terror victim state does B, then terror origin state does C, outcome (3, 4).

Terror victim state would choose outcome (3, 4), as this is better from its perspective.

- Should terror origin state move first:
    - If terror origin state does C, then terror victim state does B, outcome (3, 4).
    - If terror origin state does D, then terror victim state does B, outcome (4, 3).

Terror origin state would choose outcome (3, 4), as this is better from its perspective.

Neither terror victim state nor terror origin state has a first move, and also neither would benefit any better than the present Nash Equilibrium of (3, 4).

b. Can Terror Victim State Threaten Terror Origin State?

- Terror victim state wants, terror origin state to play D (take action against terrorists).
- If terror origin state does C, then terror victim state threatens to do A, outcome (2, 2).
- Normally, if terror origin state does C, then terror victim state does B, outcome (3, 4)
- Threat exists, as the threatened outcome hurts both the players.

- If terror origin state does D, then terror victim state does B, outcome (4, 3).
- The threat exists and works alone best, as outcome (4, 3) is better for terror victim state.

Terror victim state can threaten terror origin state to take play D (take action against terrorists).

c. Can Terror Victim State Promise Terror Origin State?

- Terror victim state wants, terror origin state to play D (take action against terrorists).
- If terror origin state does D, then terror victim state promises to do A, outcome (1, 1).

Normally, if terror origin state does D, then terror victim state does B, outcome (4, 3).

Terror victim state can't promise terror origin state, as the promised outcome would be worst for both the players.

d. Can Terror Origin State Threaten or Promise Terror Victim State?

As the present outcome is the best for terror origin state, the terror origin state would not like to threaten or promise.

Analysis of all the strategic moves, indicate that terror victim state can threaten terror origin state to play D (take action against terrorists).

3. Interval Scaling

Until now, we have only considered a scale of order of numbers (i.e., 1 is better than 2, 2 is better than 3 and 3 is better than 4), for the players in this game. However, in order to have a more meaningful analysis and outcomes, an interval scale that also caters for the ratio of differences of numbers is more

appropriate. As stated by Straffin, "a scale on which not only the order of numbers, but also the ratios of differences of the numbers is meaningful is called an interval scale."[39] While working out the absolute payoffs, it has been assumed that a small boat terror attack has not been detected and identified by the terror victim state's MDA, and this state would be in a better position compared to the terror origin state if she launches an offensive against the latter. The payoffs are based on the assumptions, and different status of terror victim state's MDA and the actual military capability of both the players could change their absolute value, but the relative hierarchy of the payoffs would be the same. The absolute payoffs have been accorded to later analyze, how the game can be tilted in the favor of the terror victim state.

- Terror victim state:
    - 10 – Best – Terror origin state takes action against the terrorists; terror victim state remains protective (as this is the best option for terror victim state).
    - 5 – Next Best – Terror origin state takes no action against the terrorists; terror victim state remains protective (since the terrorists could infiltrate the terror victim state's MDA, low absolute value of the protective stance has been accorded).
    - 4 – Least Best – Terror origin state takes no action against the terrorists; terror victim state goes offensive (considering that terror victim state would be in an advantageous position compared to the terror origin state).
    - 1 – Worst – Terror origin state takes action against the terrorists: terror victim state goes offensive (as this is the worst option).

[39] Philip D. Straffin, *Game Theory and Strategy,* The Mathematical Association of America, 1975.

- Terror origin state:
  - 10 – Best – Terror origin state takes no action against the terrorists; terror victim state remains protective (as this is the best option for terror origin state).
  - 9 – Next Best – Terror origin state takes action against the terrorists; terror victim state remains protective (considering that terror origin state would have to put in some effort to take action against its citizens).
  - 2 – Least Best – Terror origin state takes no action against the terrorists; terror victim state goes offensive (considering that terror origin state would be in a disadvantageous position compared to terror victim state).
  - 1 – Worst – Terror origin state takes action against the terrorists: terror victim state goes offensive (as this is the worst option).

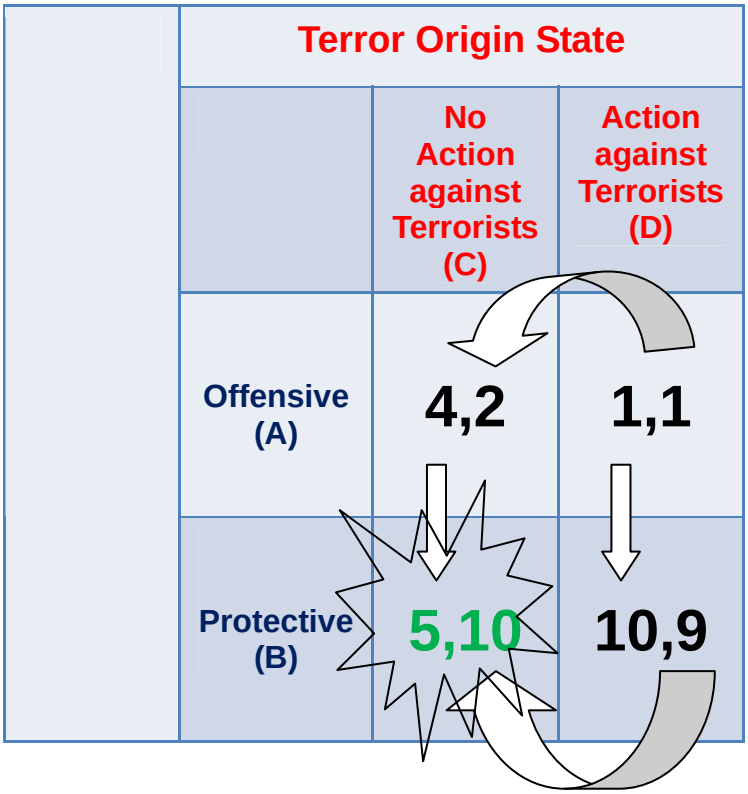

Figure 6. INTERVAL SCALED GAME

This picture, along with the analyzed strategic moves, conveys that:

- Terror origin state's pure dominant strategy is not to take action against the terrorists, and have an absolute payoff of 10 in this game.
- Terror victim state's pure dominant strategy is to remain protective, and have an absolute payoff of 5 in this game.
- Terror victim state could coerce terror origin state to take action against the terrorists, as this game has a threat and moreover since there is only slight reduction in terror origin state's payoff (i.e., from an absolute value of 10 to 9).
- Terror victim state should increase its BC Strategy's (protective strategy even if terror origin state takes no action against the terrorists) payoff, which is presently 5, by improving its MDA in territorial sea.

4. Security Level

Until now, the game has been analyzed from a pure economics standpoint, where both the players are maximizing their respective payoffs. To analyze this game from the security standpoint, the security levels of each player would also have to be analyzed. The security levels are the minimum assured payoffs for each player when the other player starts minimizing the opponent.

- Terror victim state:

Terror victim state is maximizing its payoffs, whereas terror origin state is minimizing them.

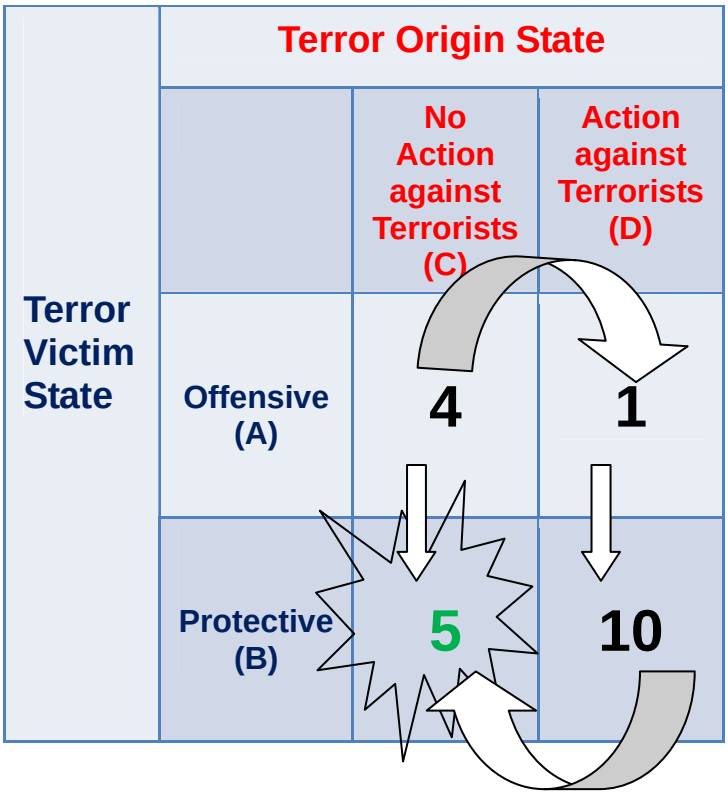

Figure 7. TERROR VICTIM STATE SECURITY LEVEL GAME

In this game, terror victim state has a security level (minimum assured payoff) of 5, and the prudential strategy is to remain protective.

- Terror origin state:

Terror origin state is maximizing its payoffs, whereas terror victim state is minimizing them.

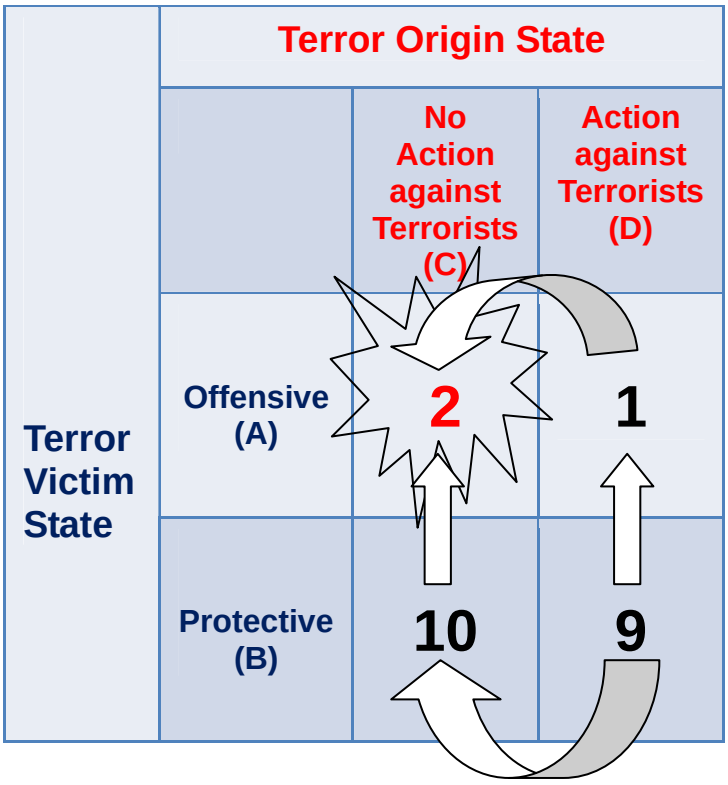

Figure 8. TERROR ORIGIN STATE SECURITY LEVEL GAME

In this game, terror origin state has a security level (minimum assured payoff) of 2, and the prudential strategy is not to take action against terrorists.

5. Nash Arbitration

Is the security level solution of (5, 2) (i.e., terror victim state's SL of 5 and terror origin state's SL of 2) Pareto optimal? An outcome is Pareto optimal, if no superior outcome exists. To further analyze the best solution from the point of both security and stability, the game is graphically represented as:

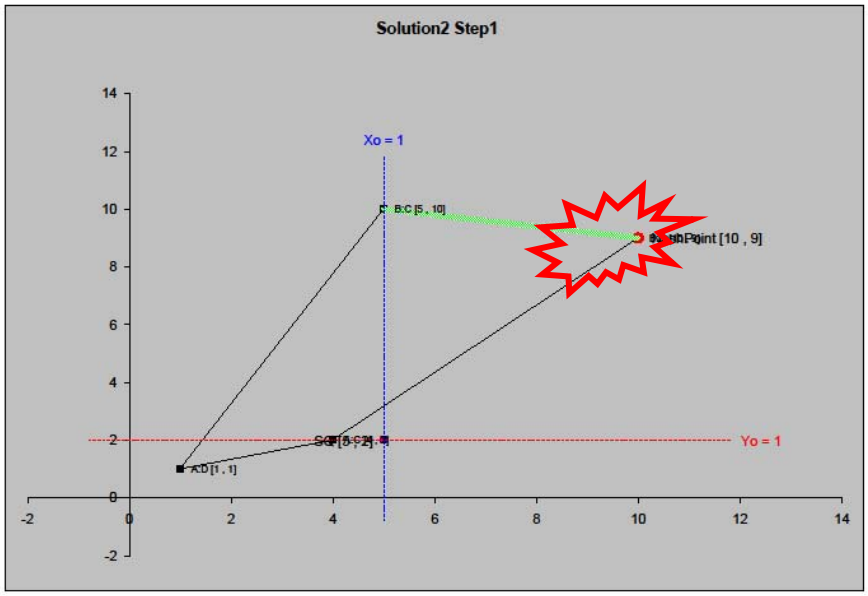

Figure 9. NASH ARBITRATION GRAPH

As can be seen in Figure 9, the present security level of (5, 2) is not a Pareto optimal solution. The Nash Point, a Pareto optimal solution of this game is (10, 9). This solution is the BD outcome of this game, implying that terror origin state should take action against the terrorists and terror victim state should continue her protective strategy. However, if the terror victim state adapts her MDA to the territorial sea by enhancing coastal surveillance against small boats; then its assumed absolute payoff of 5, would increase depending upon the effectiveness of its MDA in the territorial sea up to a maximum value of 9. This implies that the present security level of (5,2) could be changed to (9,2) by the terror victim state by enhancing its coastal surveillance against small boats. Although this is still not a Pareto optimum solution, it would place the terror victim state in a much more advantageous position to coerce the terror origin state to take action against the terrorist organizations operating from its territory or to deter the terror origin state from supporting terrorism. Even if the terror origin state does act against the terrorist organizations, a security level payoff of 9 for

the terror victim state achieved by enhancing coastal surveillance against small boats, provides an excellent strategy against the small boat terror attacks in territorial sea.

6. Conclusion

The Game theory utilized to analyze the situation of countering small boat terrorism reveals; the terror victim state can coerce the terror origin state to take action against the terrorist organizations operating from its territory or deter the terror origin state from supporting terrorism, provided the former threatens the latter with an offensive action that hurts them both and has dire consequences for the terror origin state. The terror victim state should take action as demanded by the terror victim state to improve the security and overall stability between them. However, if the terror origin state does not take action, and the terror victim state goes offensive against the former then in addition to the dire consequences faced by the terror origin state, the payoff for the terror victim state would be very high for long engagement both financially and in terms of resources including human power. The preferred option for the terror victim state should be to improve its MDA in its territorial sea for enhanced coastal surveillance in order to counter the threat of small boat terror attacks. This would not only put it in an advantageous position to coerce the terror origin state to take action against the terrorist organizations operating from its territory, but with the highest possible security level that can be achieved without the cooperation of the terror origin state, it will also provide the best strategy for the terror victim state to counter the threat of small boat terror attacks in territorial sea by enhancing its coastal surveillance.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MARITIME DOMAIN AWARENESS

A. INFORMATION ASYMMETRY

As articulated by McCormick, "insurgents always exploit the information advantage, their identity (who), place of attack (where) and time of attack (when) unknown to state; to overcome the force advantage, military power of the state."[40] Terrorists also utilize the same strategy to negate the force advantage of counterterrorism forces. Actionable intelligence, if available to counterterrorism forces, can overcome this information advantage being exploited by the terrorists, and therefore becomes the most vital requirement for a successful counterterrorism operation. "Maritime Domain Awareness is all about generating actionable intelligence, the cornerstone of successful counterterrorist and maritime law enforcement operations."[41] In order to provide actionable intelligence, MDA has to collect information from various sources and convert it into a Common Operating Picture (COP). However, in order to generate actionable intelligence in the form of COP, the clarity of the desired maritime area has to be enhanced by tagging and tracking all contacts utilizing a network of appropriate sensors. In conventional wars, navies have been able to make the battle space clearer through network centric operations, but the maritime environment in a nation's own coastal waters is cluttered with small boats almost all of which are friendly. To enhance the transparency of the desired maritime space in densely cluttered own coastal waters, a different approach from that required on the high sea is required. Enhancing the transparency of the maritime space on the high seas requires the identification of the hostile units from the neutral contacts, as the location of own units is well known; but the identification of hostile units in territorial sea would also necessitate their identification from friendly contacts, like own fishing and / or other small boats. Identification of the

---

[40] Gordon H. McCormick, *Defence Analysis Class,* Naval Postgraduate School, Monterey, July 16, 2009.

[41] Maritime Domain Awareness, GlobalSecurity.

hostile units from the friendly contacts, in addition to undertaking the same with the neutrals contacts, therefore, becomes the most fundamental requirement for enhancing the clarity of maritime space in the territorial sea. Although the fundamental of MDA at high sea and in the territorial sea (i.e., collating information for generating a COP to provide actionable intelligence) may remain the same, but the latter requires an additional capability for identifying the hostile units from friendly contacts. This capability would be like a patch, which when attached with the existing MDA would adapt it to the territorial sea. The aim of this thesis is primarily to provide this patch, which would function like a security update to computer software, fixing the existing MDA capability in order to counter the threat of small boat terrorism in the territorial sea.

B. MARITIME SPACE TRANSPARENCY

> One of the main problems in counterterrorism today is that there are so many people and vehicles, and so much data and material, moving through globalization's myriad networks that it seems virtually impossible to track it all effectively. Nowhere has this problem been more acute than on the high seas. In 2006, Adm. Harry Ulrich, then U.S. commander of NATO Naval Forces Europe, decided to do something about it. Despite having virtually no resources, his dream was to transpose the global air-traffic control system onto sea traffic. Worldwide, aircraft are transparent, because they're all required to carry an identification beacon that allows them to be tracked leaving and entering airports, and monitored between airports, by a global network of sensors. Act suspiciously and somebody's fighter aircraft will soon be on your tail. No such pervasive system currently exists globally for maritime traffic. While bigger ships carry an ID beacon similar to aircraft, without a shared monitoring network, that's like tracking only selected commercial jets and giving everyone else a pass. So Ulrich, upon taking command, asked a simple question: "If we can do that in the air, why can't we do it on the sea?"[42]

Maritime Space Transparency (MST), as used in this thesis, is the degree of transparency of the desired maritime space. Complete Maritime Space

[42] Thomas P. M. Barnett, *Great Powers: America and the World After Bush,* New York: Penguin Group, 2009.

Transparency in terms of percentage would indicate that the identity of all the contacts, with respect to their being friendly or hostile, has been established in this space. Thus, hundred percent MST would imply that the identity of all contacts has been established, and zero percent would indicate that none of them has been detected and identified. To establish the nature of all the contacts in a desired maritime space, a network of sensors should therefore be capable of detecting and identifying them. Thus, detection and identification turn out to be the two variables that govern the MST. Traditionally, contacts at sea are first detected by some equipment like radar, and thereafter, those contacts are identified by visual or other means; in such scenarios, the probabilities of detection and identification would be governed by the conditional law, as the probability of identification given the occurrence of detection. Whereas, if the AIS (which automatically broadcasts the identity of the contact without being triggered by detection) is being utilized, the probabilities of detection and identification become independent, as the probability of the radar detecting the contacts does not affect the occurrence of probability of identification by AIS. A Venn diagram of the maritime space with regard to the probabilities of detection and identification would depict as:

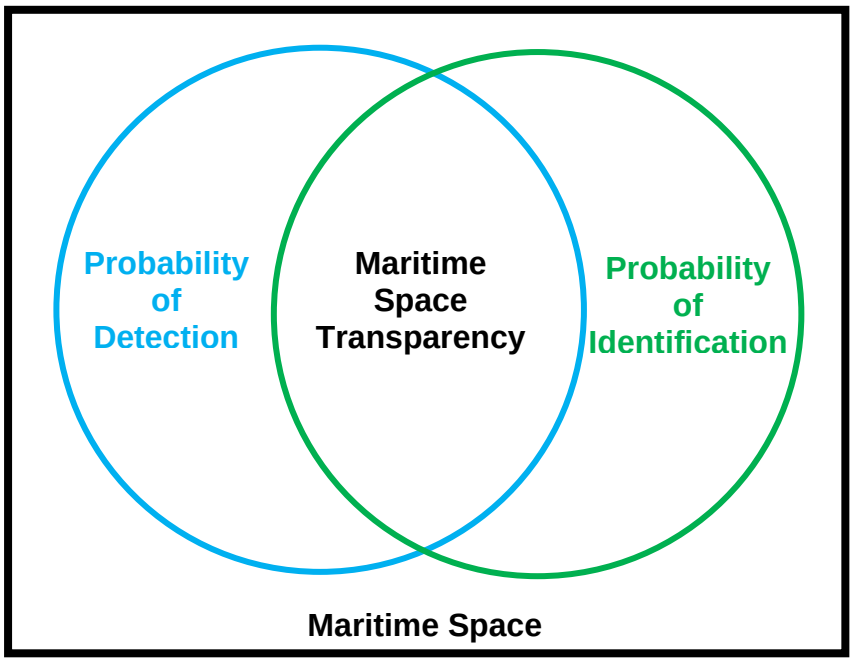

Figure 10. VENN DIAGRAM OF VARIABLES

The Venn diagram indicates that in a desired maritime space, the Maritime Space Transparency is the intersection of the probability of detection and the probability of identification of the contacts. Mathematically, this can be expressed as:

Maritime Space Transparency = P (Detection) ∩ P (Identification)

Maritime Space Transparency = P (Detection) x P (Identification)

Therefore, in order to increase the maritime space transparency, the following needs to be undertaken

- Probability of detection and the probability of identification independently needs to be increased
- Detection and identification information originating from different sensors needs to be fused to provide a greater intersection of their probabilities.
- Detected contacts not identified need to be investigated and classified as hostile or friendly to confirm their identity.

- Contacts automatically broadcasting their positions for identification but not yet detected, need to be investigated for confirming their presence.

In the preceding paragraphs, the relationship between the MST and the probabilities of detection and identification has been exhibited mathematically. In the succeeding section, the process of how Israel enhanced the MST in its territorial waters would be traced through in history to establish its efficacy for effectively countering the threat of small boat terrorism. The case study of Israel would also be utilized to identify the appropriate means of detection and identification utilized by Israel to increase their probabilities for enhancing the MST.

C. ISRAEL A CASE STUDY

Historically, Israel has immense experience in countering small boat terrorism, as this country has been combating it since 1970. It was in the 1970s, that Palestinian terror organizations started using the sea to infiltrate Israel. Three out of the four major terrorist attacks in Israel in the 1970s, i.e., Tel Aviv's Savoy hotel attack in March 1975, Coastal Road attack in March 1978 and Haran attack in April 1979, were small boat terror attacks. On 24 June 1974, the first terror attack to use the sea as a means of infiltrating Israel was undertaken by three terrorists who landed on the Naharia beach, having set sail from Lebanon. These terrorists seized several hostages in a nearby apartment building, killed four people and wounded eight, before being killed by the Israeli security forces. "Three Arab Muslim terrorists entered Israel and seized hostages in an apartment building in Nahariyya. They killed four Jews and wounded eight more before they themselves were killed in a gun battle."[43] In response to this attack, Israel attempted to enhance its MST on its northern border by setting up coastal radar station and lookouts. "The Israeli security forces, especially the navy,

43 "1974 Islamic Terrorism Timeline," *Prophet of Doom,* November 16, 2006, http://www.prophetofdoom.net/Islamic_Terrorism_Timeline_1974.Islam (accessed June 21, 2010).

increased their security measures on the northern border to prevent further infiltration, by setting up not only a radar station and lookouts at Rosh Hanikra, but also by introducing security zones in which no civilian shipping and swimming was allowed."[44] Although the coastal radar would have provided a good probability of detection, but relying only on visual lookouts could hardly have provided any probability of identification. Therefore, in addition to lookouts Israel also established a security zone, in which no civilian shipping or swimming was allowed, to facilitate classification of contacts, in order to increase the probability of identification. The concept of establishing such zones for identification has been used throughout military history, the most prominent being the Maritime Exclusive Zone and Total Exclusive Zone established by United Kingdom in the Falkland War; but the efficacy of such zones in increasing the probability of identification largely depends upon the capability of the authority promulgating it, to prevent neutral from entering this zone. Additionally, such zones can only be promulgated for a limited duration due to their effect on maritime traffic and eventual disruptive effect on the country's economy.

After the implementation of such measures in Israel's northern territorial waters, terrorist changed their tactics to circumvent these measures. On 5 March, 1975, terrorists utilized boats launched from a mother ship from the west, to land on Tel Aviv beach and attack the Savoy hotel. The Israeli Security Forces killed the terrorists, but in the process, seven hostages also lost their lives.

> On 5 March 1975, Arab terrorists landed on the Tel Aviv beach and attacked the Savoy hotel, capturing parts of the building and holding hostages. The terrorists were assaulted by the Israeli Defense Forces, most of them were killed and a number captured. But 7 hostages lost their lives. A day later, the vessel that brought the terrorists to the point where they transferred to rubber boats was seized by the Israeli navy.[45]

---

[44] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

[45] "Statement in the Knesset by Defence Minister Peres," *Israel Ministry of Foreign Affairs,* March 11, 1975, http://www.mfa.gov.il/MFA/Foreign%20Relations/Israels%20Foreign%20Relations%20since%201947/1974-1977/68%20Statement%20in%20the%20Knesset%20by%20Defence%20Minister%20Pe (accessed June 21, 2010).

In response to the Savoy hotel attack, Israel increased the number of ships and aircrafts for maritime patrols and searches, respectively, in order to enhance its reconnaissance capability in the Mediterranean Sea. While these measures may have prevented some terrorist attempts and also resulted in countering a terrorist speedboat at the Tel Aviv Marina in September 1976, they could not prevent the Coastal Road attack on 11 March 1978, which killed a total of 37 people and injured more than 70. These measures to increase the detection and identification capabilities were primarily accomplished by moving platforms such as ships and aircraft, and therefore could not provide continuous enhanced MST in the time and spatial domains.

> After the 11 March 1978, Bus Hijacking on the Coastal Road, Israel launched a major military incursion into South Lebanon, called the Litani River Operation. Israel crossed into southern Lebanon on March 15 and struck at PLO terrorist bases and staging areas south of the Litani River, up to ten kilometers deep inside the country. Twenty-one IDF soldiers were killed before the operation ended on 21 March 1978.[46]

In spite of force superiority, Israel's offensive action against Lebanon could not destroy the Palestinian terror infrastructure in Lebanon. This invasion of Lebanon only resulted in the United Nations Organization passing resolution 425 and 426, directing Israel to withdraw its forces from Lebanon and inducted United Nations Interim Force in Lebanon.

> Having heard the statements of permanent representatives of Lebanon and Israel, gravely concerned at the deterioration of the situation in the Middle East and its consequences to the maintenance of international peace, convinced that the present situation impedes the achievement of a just peace in the Middle East; United Nations Organization calls: for strict respect for the territorial integrity, sovereignty and political independence of Lebanon within its internationally recognized boundaries, upon

---

46 *Palestine Facts: What was the Litani River Operation, Israel's invasion of Lebanon in 1978,* http://www.palestinefacts.org/pf_1967to1991_lebanon_1978.php (accessed June 21, 2010).

> Israel immediately to cease its military action against Lebanese territorial integrity and withdraw forthwith its forces from all Lebanese territory.[47]

Israel with its 1970s and 1980s experience of maritime terrorism focused its maritime counterterrorism strategy more towards protective measures. As early as the 1990s, this strategy proved effective and increased the difficulty of the maritime terrorists operating against Israel.

> On May 30, 1990 Israeli security forces foiled an attempt by PLF terrorists to infiltrate Israel from the sea near Gaash and Nitzanim. Code named Al-Quds, the 16 terrorists departed from Benghazi, Libya on May 27, 1990 on a Libyan ship. Following the failed plot, the PLO announced through Kaled al-Hassan on June 4, 1990, that the PLF operation was utilizing the wrong technique "because everyone knows that Israel has stated that its radar lab can scan as far as Malta.[48]

Israel's protective strategy has been primarily two-pronged. The first level comprises of enhancing the MDA by gathering intelligence from various sources including long-range maritime reconnaissance aircraft. The second level closer to coast concentrates on increasing the MST in the time and spatial domains by deploying a network of coastal sensors.

> The first protection stage consists of intelligence gathered by the various Israeli intelligence services and the Foreign Ministry. Israel also relies on land-based aerial reconnaissance patrols (Shahaf Maritime Aircraft) and patrols conducted by Israeli naval ships (Sa'ar 4-5), in order to secure a maritime situational awareness of its western border. While the outer border of these controls is set at 100 nautical miles off the Israeli Coast, the lateral borders are specified by the territorial waters and air traffic regulations of each neighboring country. On closer range (up to 32 nautical miles) nine Israeli radar stations situated along the coast from Rosh Hanikra in the north to Erez near the Gaza Strip, provide the Central Command Center (C4I), through its three local command centers Haifa, Ashdod and the Red Sea Region, with a complete picture of

---

47 "Security Council Resolutions - 1978," *United Nations,* http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/368/71/IMG/NR036871.pdf?OpenElement (accessed June 24, 2010).

48 Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

> all maritime movements. Furthermore, these regional command centers can direct up to eleven coastal patrol boats (Mediterranean coastline), in order to intercept suspicious ships / floating objects. Following the withdrawal of the Israeli Defense Forces from the Gaza Strip in August 2005, Israel's navy found itself replacing its physical barriers and reconnaissance posts, such as Tel Ridan in Gaza, with technical sensors near the border with the Gaza Strip. These technical sensors consist of infiltration detection sensors such as the Long Range Reconnaissance and Observation System (LORROS) built by Elbit which teamed up with IAI's subsidiary Elta System's EL/M-2226 coastal surveillance radar system. EL/M-2226 is designed to detect patrol boats at ranges up to 32 nautical miles. Mounted atop 820ft.-high smokestacks at the nearby Ashkelon power station, the dual system provides the operator with a deep view into the Gaza Strip. Moreover, as part of Israel's effort to reduce spending, the Israeli Navy will replace part of its manned coastal surveillance stations with unmanned radar stations by 2008. Unmanned radar stations, stationed on high vantage points far from population centers along the coast, can be more powerful and therefore provide greater coverage and resolution.[49]

The Israeli coastal defense system utilizes a chain of nine coastal radars networked together to provide a continuous coverage of up to 32 nautical miles from the coast for 24 hours each day every week round the year (24/7/356). These radars have special features like Inverse Synthetic Aperture (ISA) function to generate two-dimensional high-resolution images of the targets. This feature provides target discrimination capability by measuring the dimensions (extent and height) of the target. Though the extent of the target would depend upon its aspect, the Inverse Synthetic Aperture tool could be utilized effectively to differentiate between small, medium and large targets. The radars are primarily utilized for detection, but the Inverse Synthetic Aperture feature does provide limited identification capability.

Post-9/11 terror attacks, the International Maritime Organization to counter the threat of maritime terrorism adopted International Ship and Port Facility Security (ISPS) Code in 2002. This regulation mandated the fitment of the AIS on all ships of 300 tons and more by 31 December 2004.

---

[49] Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

> In 2000, IMO adopted a new requirement (as part of a revised new chapter V) for all ships to carry automatic identification systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically. The regulation requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The requirement became effective for all ships by 31 December 2004. [50]

This system is designed to automatically provide the ship's identity, position, course and speed to other ships, aircrafts and shore stations, however the warships, government vessels, fishing vessels and vessels smaller than 300 tons are exempted from the fitment of the AIS. As per the existing regulations, this system without any further enforcement by the coastal state cannot be utilized for identifying small boats. To improve the probability of identification of its coastal defense system, Israel mandates that all ships and small crafts, when within 100 nm and 25 nm respectively from Israeli coast, should have their AIS activated.[51] Any ship or craft that does not meet this requirement, is further classified by long-range day and night shore based, Unmanned Aerial Vehicle (UAV) and Unmanned Surface Vehicle (USV) fitted optical sensors. The Israeli coastal defense system thus maintains an enhanced MST 32 nautical mile from its coastline, by utilizing radars, AIS, and day and night electro optical sensors. Their networking on a common grid ensures optimum data fusing for a greater intersection of the probabilities of detection and identification, to enhance MST. Additionally, contacts that have been detected and not identified are further investigated with shore-based, Unmanned Aerial Vehicle (UAV) and Unmanned Surface Vehicle (USV) fitted with day and night electro-optical sensors, to ensure the near-complete intersection of the detection and identification probabilities.

---

[50] *IMO adopts comprehensive maritime security measures,* December 13, 2002, http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689 (accessed January 22, 2010).

[51] *State of Israel Ministry of Transport and Shipping,* http://en.mot.gov.il/index.php?option=com_content&view=article&id=145:rad17m&catid=17:noticetomariners&Itemid=12 (accessed January 30, 2010).

Unlike the Israeli Heron UAV, which can carry a multiple sensor payload, such as radar and / or electro optical sensors; the Israeli Navy's Protector USV is only fitted with electro-optical sensor and a laser range finder. The platforms that are fitted with only electro-optical sensors have to utilize the radar inputs from the coastal defense network in order to be integrated into this network.

In July 2006, a senior Israeli navy officer told CNN, that "there have been 80 maritime terror plots that Israel has detected over the years and most of them have been foiled, since Israel has established an elaborate network of early warning devices to monitor the threats from the sea."[52]

D. CONDITIONALITY

If Israel has been able to enhance its MST in and around the territorial waters, then why has not this concept, especially the utilization of the AIS for increasing the probability of identification, been incorporated by other nations as well? Could there be a conditionality that needs to be satisfied for pragmatically implementing the concept of utilizing the AIS with radar for enhancing Maritime Space Transparency? Many countries, including the United States, are considering the fitment of AIS on small boats as well.

> While many organizations are involved in port security — from private firms to local authorities — is it ultimately the U.S. Coast Guard's responsibility. "We've taken a series of steps to reduce vulnerability and I think we've got to keep going in that direction," U.S. Coast Guard Admiral Thad Allen said. The service in December published a "notice of proposed rule making" that would require commercially operated craft more than 65 feet long and vessels transporting more than 50 people to carry the Automatic Identification System — a communication transponder that identifies a vessel's position, speed, destination and cargo. It is currently required only in craft weighing more than 300 gross tons.[53]

---

[52] *CNN Transcripts,* July 28, 2006, http://transcripts.cnn.com/TRANSCRIPTS/0607/28/sitroom.02.html (accessed Jun 21, 2010).

[53] Matthew Rusling, "No Silver Bullet for Thwarting Terrorists Aboard Small Boats," *National Defense Industrial Association,* March 2009, http://www.nationaldefensemagazine.org/archive/2009/March/Pages/NoSilverBulletforThwartingTerroristsAboardSmallBoats.aspx (accessed June 30, 2010).

In addition to Israel, Singapore also has a very similar coastal defense concept, which amalgamates the inputs from the radar and AIS, and also utilizes electro-optical sensors for further classification of certain contacts. Importantly, the fitment of AIS is currently compulsory for all vessels including small crafts, in the territorial waters of Singapore and also in the Singapore Straits. These transponders are called Harbor Craft Transponder System (HARTS) and they automatically send the vessel's identification, position, course and speed to port authority.

> Singapore will require small harbor and pleasure craft to be fitted with transponders as part of security measures to counter terror and piracy threats, the Maritime and Port Authority (MPA) said Friday, July 1, 2005. The MPA said the Harbor Craft Transponder System (HARTS) has been developed for use by smaller vessels outside the coverage of security rules mandated by the International Maritime Organization (IMO) which covers bigger ships. The transponders will enable the vessels to transmit their identity, position, course and speed to authorities onshore. They will also contain a 'panic button' to alert land-based authorities in the event of a security threat.[54]

The ranges of the AIS, radar and optical sights are limited to line of sight; therefore, setting up coastal defense based on these systems would require a large number of such coastal sensors for countries with longer coastline. Since Israel and Singapore have limited coastlines, these countries have been able to establish such good coastal defense systems with enhanced MST. The extent of the coastline and / or the maritime space in terms of square nautical miles therefore is an environmental variable, when attempting to enhance the MST. According to the historic analysis of maritime terrorism in Israel, analysis of Israeli coastal defense and the corroboratory evidence of Singapore harbor; it can be summarized that MST for coastal defense in and around the territorial waters can be enhance by amalgamating the radar (for detection), AIS (for identification), and day and night electro-optical sight (for further classification)

---

[54] Agence F. Presse, "Singapore beefs up maritime security, installs transponders on small vessels," *Singapore Windows,* July 01, 2005, http://www.singapore-window.org/sw05/050701a1.htm (accessed July 01, 2010).

inputs, by networking these sensors. While undertaking coastal defense with such sensors, the extent of the coastline and / or size of the maritime space would be vital environmental conditions. The available technologies, which could be adapted to enhance the MST around longer coastlines and in larger areas, utilizing such sensors, would be examined in the next chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. MARITIME SPACE TRANSPARENCY

A. LARGE MARITIME SPACE

As detailed in the previous chapter, Maritime Space Transparency in and around the territorial waters in order to effectively counter the threat of small boat terrorism, has been enhanced by few nations including Israel and Singapore. The primary means of detection and identification utilized by these countries include coastal surveillance radar, such as Elta System's EL/M – 2226,[55] and AIS[56] respectively. The coastal surveillance radars, like Elta System's EL/M – 2226, are optimized for detecting small boats, and therefore operate in "X" Band radar frequency (8 -12 GHz).[57] The AIS as mandated by the International Maritime Organization with an effective date of 31 December 2004, on all ships of 300 tons and more, operates on the VHF radio frequency (30 – 300 MHz). "The AIS is a shipboard broadcast system that acts like a transponder, operating in the VHF maritime band that is capable of handling well over 4,500 reports per minute and updates as often as every two seconds."[58] The limitation of both these systems is their Line of Sight ranges; therefore, even if the power of these systems was increased their ranges would still be limited to the horizon. The radar detection range depends upon many factors, such as transmitter power output, receiver sensitivity, beam forms, antenna type, signal processing, atmospheric conditions, etc; however, the horizon range is a major criterion while establishing the maximum achievable range of the radar.

> Under standard atmospheric conditions, the radar beam tends to bend slightly downward, and the distance, d, of the radar horizon is given by the formula:

---

55 Akiva J. Lorenz, "The Threat of Maritime Terrorism to Israel."

56 *State of Israel Ministry of Transport and Shipping.*

57 *IAI ELTA System Ltd,* http://www.iai.co.il/sip_storage/files/2/36842.pdf (accessed July 01, 2010).

58 *U.S. Department of Homeland Security - AIS.* http://www.navcen.uscg.gov/?pageName=AIS (accessed July 01, 2010).

d (in n miles) = 1.22 √h (in feet) or

d (in n miles) = 2.21 √h (in meters),

where h is the height of the antenna in feet or meters.

Thus, the theoretical radar horizon range based purely on the antenna and the target heights is given by the formula:

Rd = 1.22 √h (ft) + 1.22 √H (f) or

Rd = 2.21 √h (m) + 2.21 √H (m),

where, h and H are the heights of the antenna and targets respectively in feet or meters. In both cases Rd is the theoretical detection range in nautical miles.

This relationship is theoretical since it assumes:

- Standard atmospheric conditions.
- Radar pulses are sufficiently powerful.
- Target response characteristics are such as to return detectable response.
- Weather condition, such as precipitation, etc., through which the pulses are to travel, will not unduly attenuate the signal.[59]

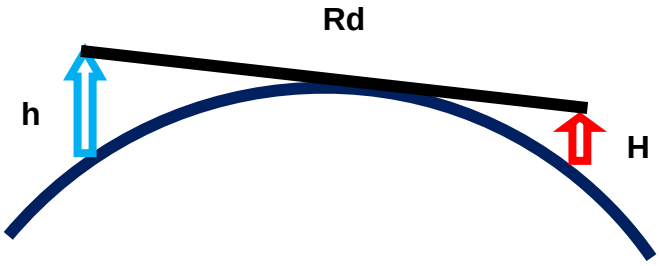

Figure 11. RADAR HORIZON RANGE

[59] Alan Bole, Bill Dineley and Alan Wall, *Radar and ARPA,* Burlington: Oxford, 2005.

The horizon range thus depends upon the target and antenna heights. Since the target height is not a controllable variable, the horizon range can only be increased by increasing the height of the antenna. The concept of covering a larger maritime space by increasing the height of the antenna in order to enhance the horizon range has been and is being utilized in the maritime environment by positioning coastal surveillance radars on hilltops and also by deploying aircrafts for maritime reconnaissance. Both these options have certain drawbacks, if they need to be utilized for maintaining continuous surveillance in time and spatial domains. The topography of the coastline may not always have the hill of the desired heights at required distance to provide in-depth coverage of maritime space with sufficient inter radar overlap. Therefore, the concept of positioning radar on hilltops may be a good option for limited coastline surveillance in hilly coastal terrain, but may not be viable for covering longer coastline with flat topography. Regarding the utilization of aircraft for increasing the antenna height, there are many recommended searches and patrols for maritime reconnaissance based on various operational analysis methods, but all these can only provide near-continuous coverage in time and spatial domains due to the mobile nature of this platform. Though one can argue that the option of increasing the number of aircrafts for providing continuous coverage always exists, this option would not be economically viable for continuously monitoring large maritime space 24 hours a day, every week, year-round (24/7/365). To have continuous coverage in time and spatial domains of a larger maritime space, with respect to what the coastal stations can cover, a stationary aerial platform would be a preferred option. For an aerial platform to be stationary with respect to a particular point on earth, it either has to be tethered to the ground or its orbit must be synchronous with the rotation of the earth. Based on the existing technology, an aerostat and / or a geosynchronous satellite could be the two options that could be explored for enhancing the transparency in large maritime space.

B. DETECTION

1. Aerostat

Aerostat are large balloons, which are made lighter than air using helium to stay aloft and are tethered to the ground with a cable that can also provide power. A variant of an aerostat is an airship, which is traditionally manned and uses engines to fly. Since enhancing the transparency of larger maritime space continuously in time and space domain require stationary aerial platform, the airship will not be further discussed. Historically, aerostats have been utilized and are being utilized for military surveillance over land; their use along the coast for maritime surveillance therefore could be a viable option.

Figure 12. TACTICAL AEROSTAT

> The most well established LTA platform today is the Tethered Aerostat Radar System (TARS) that has been operating since 1980 along the southern United States border and in the Caribbean. Currently, TARS' primary mission is surveillance for drug interdiction. Each aerostat can lift 2,200 lbs of sensors to a height of 12,000 feet, and can detect targets out to 230 miles. The aerostat can stay aloft for months. In response to on-going threats to U.S. troops deployed to Afghanistan and Iraq, the Army has deployed small aerostats, equipped with ground surveillance sensors, to those countries. The Rapidly Elevated Aerostat Platform (REAP) was jointly developed by the Navy and the Army. This 25-foot long aerostat is much smaller than TARS, and operates at 300 feet above the battlefield. It is designed for rapid deployment and carries daytime and night vision cameras. The Army has also reportedly deployed a Rapid Aerostat Initial Development (RAID) system to Afghanistan. This aerostat is approximately twice the size of REAP and operates at approximately 1,000 feet. It also carries a suite of day and night cameras for force protection. RAID is a spinoff of the Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS) program.[60]

Presently, tethered Aerostats are fitted with surveillance and communication suites; to provide low-level radar surveillance, wider optical surveillance and communication relay capability. The United States has deployed aerostats along its southern border in the states of Arizona, New Mexico, Texas and Florida to provide low-level radar surveillance data in support of federal agencies involved in the nation's drug interdiction program.[61] Additionally, these aerostats also provide "the North American Aerospace Defense Command with low-level surveillance coverage for air sovereignty in the Florida Straits."[62] ILC Dover and Tethered Communications L.P. have manufactured these aerostats, and they are fitted with Lockheed Martin radar. These aerostats are capable of

---

[60] Christopher Bolkcom, *Potential Military Use of Airships and Aerostat,* CRS Report for Congress, CRS Web, 2005.

[61] *U.S. Air Combat Command,* http://www.acc.af.mil/library/factsheets/factsheet.asp?id=2359 (accessed July 07, 2010).

[62] *U.S. Air Combat Command.*

carrying payloads of 1,200–2,200 pounds up to 15,000 feet. The radar horizon range of the aerostats for a four-feet height target based upon the formulae discussed would be:

Rd = 1.22 √h (ft) + 1.22 √H (f)

= 1.22 √15000 + 1.22 √4

= 151.5 nautical miles at aerostat height of 15,000 feet

= 136.1 nautical miles at aerostat height of 12,000 feet

Considering these radar horizon ranges, a single tethered aerostat fitted with surveillance radar at a height of 15,000 feet, can cover a coastline of more than 300 nautical miles and provide all around maritime surveillance to a distance of more than 150 nautical miles against a four-foot high target. Traditionally, aerostats have always been considered a fair weather asset, but a modern aerostat at 15,000 feet can operate in winds of more than 60 knots, and can be hauled in or out within half an hour.

> Modern aerostat can lift a payload of greater than 3000 pounds (1364 kg) to altitudes of 15,000 ft (4.5 km) or more above sea level. They can operate in winds in excess of 60 knots (111 km/hr), and can survive winds substantially in excess of this value while moored on the ground. Winch systems and aerostat pressurizing systems have been developed that permit inhaul and outhaul at rates in excess of 600 feet per minute (183 meters/ minute). Launch and recovery operations are largely automated, but are normally monitored by a flight controller who can override the automated system.[63]

If the weather conditions obviate the deployment of aerostat, such conditions would also severely affect the survivability of small boats at sea and in turn hamper the mission of small boat terrorists. Additionally, if strong intelligence is available on some small boat terror activity, then the short absence of the tethered aerostat in very bad weather could be substituted with maritime aircraft search and / or patrol by ships. “Blowdown” is another limitation of tethered aerostats. “All tethered balloons are subject to “blowdown,” a term that

63 Nejat A. Ince, Ercan Topuz, Erdal Panayirci and Cevdet Isik, *Principles of Integrated Maritime surveillance System,* Norwell: Kulwer Academic Publisher, 1999.

refers to the downward excursion from the ground tether point. Blowdown can be considerable (two nautical miles or more) for high-altitude aerostats in high winds."[64] This drawback of a tethered aerostat can also be easily corrected by incorporating the requisite position correction by installing a GPS onboard the aerostat. Therefore, notwithstanding the limitations of tethered aerostat, these platforms can very effectively be utilized for monitoring large maritime space.

2. Satellites

It is unquestionably the best solution to utilize geosynchronous satellites to monitor large maritime space continuously in time and spatial domains; but these satellites are positioned 22,300 miles (35,900 km) above the equator. These satellites because of their heights are primarily used for weather forecasting, satellite television, satellite radio and other types of global communications; with the existing technologies it is not feasible to detect ships at sea utilizing the geosynchronous satellites. However, the efficacy of utilizing Low Earth Orbit (LEO) satellites could still be considered, as a great deal of research on utilizing a constellation of these types of satellites for maritime surveillance is underway.

> When the interest goes well beyond one's own restricted coastal waters and covers broader ocean regions or indeed becomes global then the use of space borne sensor is indispensable. For an all weather capability and with a resolution of some 10-20 meters which is independent of range, the sensor to be used would be synthetic aperture radar (SAR). SAR satellites typically orbit the earth in 100 minutes, while the earth is rotating with a speed of 15 degree/hour. This means that the successive satellite passes drift westward by 25 degree and that the coverage (in terms of average number of useful orbit per day) at a given location by one single satellite will be quite small, and totally dependent on the swath width of the SAR applications requiring frequent visits to a given area of some size would necessitate the use of multiple satellites which could be very costly. Table 2, shows the coverage capability

[64] Nejat A. Ince, Ercan Topuz, Erdal Panayirci and Cevdet Isik, *Principles of Integrated Maritime surveillance System.*

(average number of useful satellite passes per day) at three different latitudes for swath widths of 100, 200 and 400 km:[65]

	Swath Width (Km)			
Latitude (degree)		100	200	400
	0	0.07	0.14	0.28
	35	0.09	0.18	0.36
	65	0.18	0.36	0.72

Table 2. LOW EARTH ORBIT SATELLITE SAR SWATH WIDTH (FROM PRINCIPLES OF INTEGRATED MARITIME SURVEILLANCE SYSTEM)

But even if a desired coverage of a fixed location can be achieved, there is a possibility of objects going undetected because they can move out of the area of interest before the satellite comes. One therefore has to compare the sweep width with the speed of the moving objects. Table 3, shows the time needed to move across a swath of 100, 200 or 400 Km width at speed of 1, 4 or 16 knots:[66]

	Swath Width (Km)			
Vessel Speed (knots)		100	200	400
	16	3.5 h	6.9 h	14 h
	4	14 h	28 h	56 h
	1	56 h	111 h	222 h

Table 3. LEO SATELLITE SAR SWATH WIDTH V/S TARGET SPEED (FROM PRINCIPLES OF INTEGRATED MARITIME SURVEILLANCE SYSTEM)

It can be observed from Table 2 that the coverage values at the equator and mid latitude are very similar, but they increase rapidly at higher latitudes. This data implies that at 35 degree latitude, a satellite with 200 km swath width synthetic aperture radar would only be able to cover a 200 km wide area out of the 1111 km wide maritime space once a day, and in order to cover this wide maritime space once a day, at least six such satellites would be required. While a

65 Nejat A. Ince, Ercan Topuz, Erdal Panayirci and Cevdet Isik, *Principles of Integrated Maritime Surveillance System.*

66 Ibid.

wider swath width to reduce the number of satellites would be preferable from a coverage point of view, this would compromise the detection capability of synthetic aperture radar satellite. The number of satellites needed to cover a 1111 km-wide maritime space every day might look alarming, but in this configuration a constellation of six satellites in the same orbital plane would be able to cover almost the whole earth at 35 degree latitude once every day, as the adjacent 911 km gap out of the 1111 km would be equally covered by the remaining five satellites in the same orbital plane. It can also be observed from Table 3 that a revisit time of less than 14 hours is required to prevent an object crossing a swath width of 400 km undetected. Accordingly, if a greater number of such satellites is positioned in a different orbital plane in a constellation of SAR LEO satellites in order to reduce the revisit time of the desired maritime space to less than 14 hours then a vessel steaming at less than 16 knots cannot travel a distance of more than 400 km without being detected. Alternatively, if the swath width of the satellite constellation is increased, then also the revisit time of such satellites can be increased to 24 hours for the same requirement of target speed. Therefore, although a constellation of synthetic aperture radar low earth orbit satellites in a configuration to cover the complete earth once a day may not be able to provide continuous detection capability for the desired maritime space, it can certainly enhance the overall MDA capability.

In December 2007, MacDonald, Dettwiler and Associates Ltd, (MDA), Canada, launched RADARSAT-2, which provides the world's most advanced commercially available C-band radar imagery. RADARSAT-2 is an important new data source of global geospatial intelligence. It offers very specific capabilities, the advantages of multi-polarized Synthetic Aperture Radar, and applications of its specialized image products for defense and intelligence communities. RADARSAT-2 data has significant potential to play a key role in support of international MDA. RADARSAT-2's Ultra-Fine beam mode (3-m resolution)

improves ship detection and, in combination with fully polarimetric (Quad-Pol) data, offers the potential for ship classification. Figure 13, shows a port scene with ship detection and classification.[67]

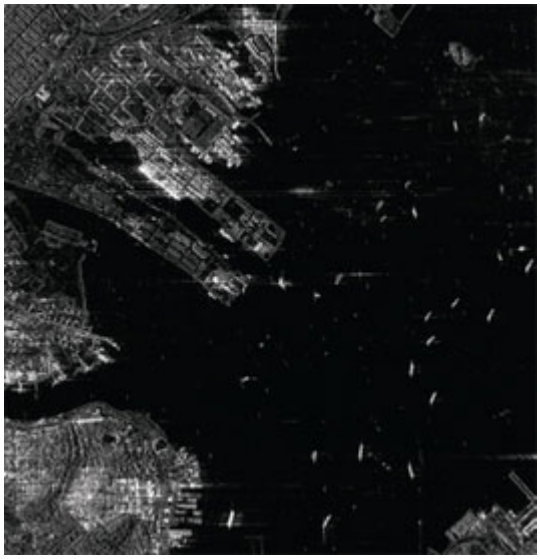

Figure 13. RADARSAT PICTURE

Based on the performance of the RADARSAT-1 and RADARSAT-2, Canada has planned to launch a constellation of LEO satellites fitted with SAR, called the RADARSAT Constellation Mission (RCM). The first satellite of this constellation is scheduled to be launched in 2012. In addition to the SAR, these satellites would also be fitted with AIS receiver.

> The successor (and complementary) mission to RADARSAT-2 will be the RADARSAT Constellation Mission (RCM), consisting of three (small) spacecraft. The overall objective of RCM is to provide C-band SAR data continuity for the RADARSAT-2 users, as well as adding a new series of applications enabled through the constellation approach. The SAR imagery is required by various Canadian government users at frequent revisit rates (high temporal resolution). The main uses of the RCM data are expected to be in the areas of maritime surveillance/security, including ship detection, and resource management. The three-satellite configuration will

67 "RADARSAT-2," *Imaging Notes,* Fall 2008, http://www.imagingnotes.com/go/article_free.php?mp_id=147 (accessed August 24, 2010).

> provide complete coverage of Canada's land and oceans offering an average daily revisit at 50 m resolution, as well as a significant coverage of international areas for Canadian and international users. It will also offer average daily access to 95% of the world. The satellites will be interoperable, enabling tasking from one satellite to the next and will be equally spaced in a 600 km low earth orbit. The constellation has a flexible design, allowing up to six satellites to fly in the same plane.[68]

If LEO satellite constellation is restricted only to SAR, then the processing time depending upon resolution may take hours for the MDA to provide actionable intelligence. However, if AIS's receiver is also fitted onboard such satellites and the data of both these sensors is fused together, then certainly actionable intelligence to guide other platforms, such as aircraft and UAV, can be generated from these MDA inputs.

C. AUTOMATIC IDENTIFICATION SYSTEM

Automatic Identification Systems are fitted on ships above 300 tons for automatic identification and navigational safety; these systems electronically exchange data with other ships and shore Vessel Traffic System (VTS). Post-9/11, the International Maritime Organization mandated the fitment of this system on all ships of 300 tons and above by 31 December 2004 to counter the threat of maritime terrorism.[69] This system automatically broadcasts the ships information, including its identity, position, course, speed, rate of turn, destination, estimated time of arrival (ETA) at destination, time of report and various other navigational information, at regular interval via a VHF transmitter.

---

68 "RCM (RADARSAT Constellation Mission)," *eoPortal,* http://www.eoportal.org/directory/pres_RCMRADARSATConstellationMission.html (accessed August 24, 2010).

69 *IMO adopts comprehensive maritime security measures,* December 13, 2002, http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689 (accessed January 22, 2010).

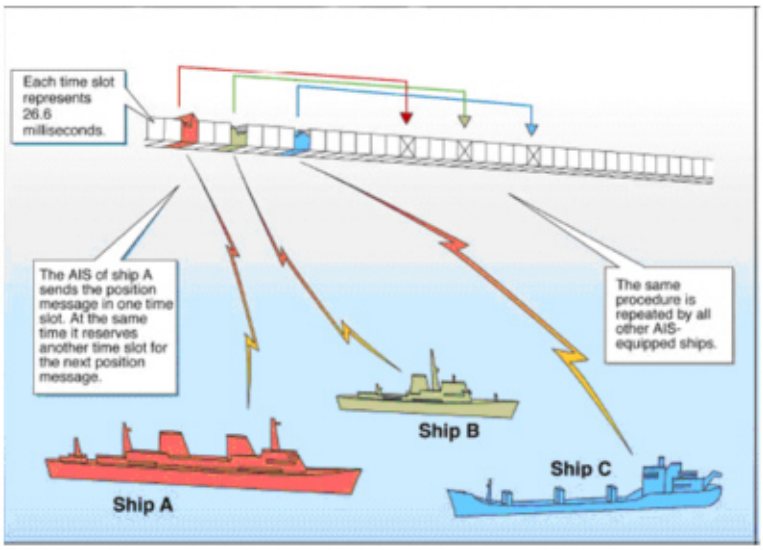

Figure 14. AIS SOTDMA DEPICTION

The AIS utilizes Self Organized Time Division Multiple Access (SOTDMA) technology to automatically form networks between ships and others receivers and this obviates the chances of data collision between various transmissions. The TDMA part of the technology divides the transmissions into 2250 time slots every 60 seconds on two different predetermined VHF frequencies, thereby providing 4500 time slots every minute.[70] The self-organized capability allows each transmitter to automatically determine its transmission slot based upon the transmission history and predicted slot allocation. These systems continuously synchronize themselves with each other to prevent the overlap or collision of data from different transmitters. In this way, when within VHF radio range of each other new stations automatically keep joining the network and the slots of the old stations are reallocated. However, in the case of contact overload in a single network, contacts further away are dropped to give preference to closer ones. Therefore, though the capacity of the system may appear to be 4500 stations, but practically it is unlimited, allowing the formation of numerous networks. In order to further optimize this system vessels that are stationary and movingly slowly transmit less frequently than those that are moving faster or are

70 *U.S. Department of Homeland Security - AIS.*

maneuvering. Vital information like identity, position, course and speed are transmitted every 2–10 seconds depending upon the vessel speed and every three minutes for stationary stations, and the additional information is broadcasted every six minutes. AIS information can be displayed on an electronic chart, as shown in Figure 15.

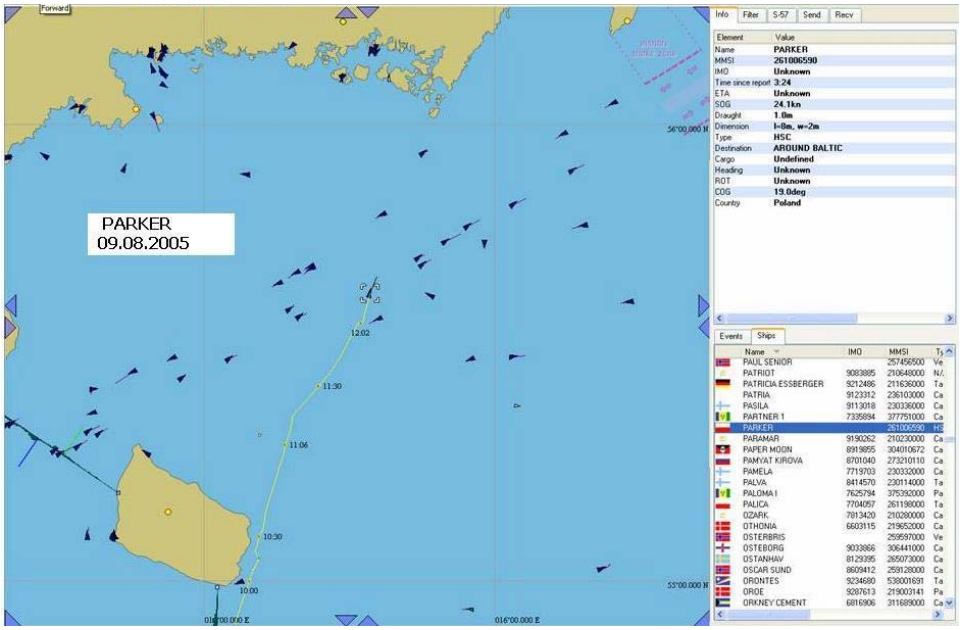

Figure 15. AIS TRACKS ON ECDIS

As can be observed from Figure 15, the identity and various other information is displayed in the bottom right window. Alternatively, the picture can also be displayed with the name of the vessels being displayed adjacent to the track on the electronic map. Since the data is in an electronic format, it can also be fused with the output of the radar; and the contacts detected on radar as not having an AIS response could be displayed as red color tracks, instead of green color for tracks with both the responses.

1. Automatic Identification System on Small Boats

The Boat Owners Association of the United States has slammed proposals from the U.S. House of Representatives Coast Guard Committee for airplane transponders to be fitted to millions of small vessels to prevent waterborne attacks. Boat U.S., in its December

> 9, 2009 address to the body, said that fitting transponders, similar to those used in aviation for monitoring by air traffic control towers, was not a practical idea and would do little to mitigate terrorism or piracy. Marine Automatic Identification Systems (AIS) have long been used as a collision avoidance tool for commercial ships and provides important vessel identification, position, speed and course information to fellow mariners as well as land-based vessel traffic control systems. Since 9/11, the Coast Guard has been tasked by the Department of Homeland Security to develop a small boat threat assessment and strategy to reduce the possibility of small watercraft being used by terrorists. "The challenge with AIS is that it does not provide the ability to reduce the small boat threat," said Boat U.S. Vice President of Government Affairs, Margaret Podlich. "Even if a would-be terrorist would go to the trouble of complying with an AIS requirement, they would merely have to pull the AIS unit's electrical plug moments before the attack," Podlich reasoned. She also mentioned a terrorist could simply steal a boat. "AIS does not recognize if people aboard a vessel are on a watch list." In addition, AIS can be easily "spoofed," or manipulated to make every AIS transponder in a certain area report inaccurate data, she concluded.[71]

As can be noted from the above citation, the fitment of AIS on small boats for countering the threat of terrorism is being deliberated in various forums. The major concern of these deliberations is that terrorists definitely would not transmit their identity, as they always exploit the information advantage to overcome the force advantage. This concern could be divided into three logical issues that need to be addressed when utilizing this system to counter terrorists. First, what if the terror boat does not comply with the fitment of the AIS or switches off this system? Second, what if the terrorists spoof their boat's identity as some other friendly boat? Last, what if terrorists utilize a hijacked friendly boat? The first issue of detecting boats not transmitting on the AIS can be resolved by fusing the outputs of the radar and AIS. Thus, a contact detected on radar without AIS output becomes alarming and would require further investigation. As mentioned earlier, an example of this could be a change in the color of the tracks between

---

[71] Mike Godfrey, *U.S. Boat Association Reproaches Small Boat Tracking Proposals,* December 16, 2009, http://www.tax-news.com/asp/story/story_marine.asp?storyname=40704 (accessed March 02, 2010).

red and green on electronic charts based on data fusion of the radar and AIS outputs. The second and third issues are the most complicated, but can be resolved by maintaining a real-time database of all friendly contacts at sea, wherein it is mandatory for all friendly units proceeding to sea to log into this database based on security token, pass phrase and geographic location based multi-factor authentication, and then follow a precommitted schedule. An example of this would be, every vessel fitted with AIS leaving certain harbor would have to commit to a certain route or area of operation by logging into the real-time database of friendly contacts system by smart card, password based encryption key and its GPS based geographic location. Now, if the terrorists try to spoof the identity of some friendly boat that is not logged into this real-time database, then the spoofed contact would be indicated as hostile. Likewise, if they spoof the identity of an already logged-in contact, then both the contacts become suspect. Additionally, if the logged in contacts do not follow their precommitted schedule of a route or an area, then these contacts also become suspicious. Such suspicious contacts would also be displayed as red color tracks. The system could also be provided with an emergency alarm button to report a hijacking or threat, and thus would also function in the manner of a friendly neighborhood-watch alarm. This system would function like information nodes operating from a fleet of friendly fishing boat reporting suspicious contacts.

If the decision is made to fit the AIS on small boats in order to enhance MST, then the next logical question is: can all vessels, irrespective of their size, which would also include small sail boats, rubberized outboard motor fitted boats, oar-boats, etc., be fitted with this system? No logical solution to this problem has so far been answered, and thus, the mandate of International Maritime Organization for fitting of AIS on all ships of 300 tons and above is the last policy decision on this issue.[72] In order to enhance the MST, and also to resolve all issues regarding the fitment of this system; this thesis proposes a role-based fitment policy for the AIS, as opposed to the existing size based policy. This

[72] *IMO adopts comprehensive maritime security measures,* December 13, 2002.

would imply that fitment of the AIS should be mandatory for all vessels proceeding outside the contiguous zone or territorial sea (in the absence of contiguous zone) irrespective of the size of the vessel. The limit of territorial waters and contiguous zone has been recommended, as it is only in the former that a country exercises sovereign jurisdiction and in the latter that country exercises the control necessary to prevent infringement of its customs, fiscal, immigration or sanitary laws and regulations within its territory or territorial sea, in accordance with the United Nations Convention on the law of the Sea.[73] A policy like this would ensure that very small vessels, which due to the nature of their role, do not cross the contiguous zone or territorial sea (in the absence of contiguous zone) of a country into the international sea would be exempted from fitment of the AIS. These are also those vessels, like small sail boats, rubberized outboard motor fitted boats, oar-boats, etc, which due to the nature of their construction do not permit the promulgation of a policy for mandatory fitment of AIS on all vessels at sea. However, an identification zone of 40–80 nautical miles, accounting for an interception capability of 2–4 hours against a 20 knots target, would have to be ensured outside the contiguous zone to permit exempting the fitment of identification equipment on vessels operating in the territorial waters and contiguous zone. Countries sharing the limit of their territorial waters could mutually work out an identification zone on either side of this limit based on their enforcement capability.

2. AIS's Aerial Monitoring

> When shuttle astronauts Michael Foreman and Randolph Bresnik flew to the International Space Station during Thanksgiving last year (2009), they attached an Automatic Identification System antenna to the Columbus laboratory so the European Space Agency could begin testing a pair of AIS receivers for use in tracking global maritime traffic from space. An AIS antenna was installed on the International Space Station late last year to test vessel tracking from space. Designed to pick up signals from standard shipboard AIS transponders, satellite-based AIS promises

73 "United Nations Convention on the Law of the Sea - Part II," *United Nations websites.*

to add a new dimension to maritime security and vessel tracking by extending ship-to-shore AIS coverage from the coast to the oceans. AIS were developed for collision avoidance and vessel-traffic management in busy ports and along coastal shipping routes, and until recently, it was terrestrial-based only. Ship transponders send VHF signals ship to ship and from ships to coastal towers and buoys, their range limited to line of sight — typically 20 to 40 nautical miles, depending on antenna height. Satellite-based AIS is feasible because VHF signals can travel the 400 or so miles into space to reach a low-Earth-orbiting satellite. The satellite receives the signal, and then forwards it to a ground station. From orbit, an AIS receiver has a range of more than 1,000 nautical miles in any direction to the Earth's horizon. Dana Goward, director of the U.S. Coast Guard's assessment, integration and risk management office, the man who oversees the agency's vessel-tracking capabilities, says the U.S. Coast Guard already is using satellite-based AIS to collect information about vessels around the world, though the coverage is neither continuous nor worldwide. U.S. Coast Guard buys its coverage from Orbcomm of Fort Lee, N.J., the only commercial provider of satellite-based AIS, with two AIS-equipped satellites in orbit. That soon will change. Between now and 2012, Orbcomm plans to launch 18 more satellites with VHF data communication capabilities, including receiving and forwarding AIS. Orbcomm's satellites circle the globe every 100 minutes. Once its constellation of 18 AIS satellites is in place, the company will be able to deliver AIS reports from a particular ship every 15 minutes, says Orbcomm CEO Marc Eisenberg.[74]

[74] "Satellite-Based AIS: One Giant Leap for Vessel Tracking," *Boats,* June 06, 2010, http://features.boats.com/boat-content/2010/06/satellite-based-ais-one-giant-leap-for-vessel-tracking/ (accessed August 24, 2010).

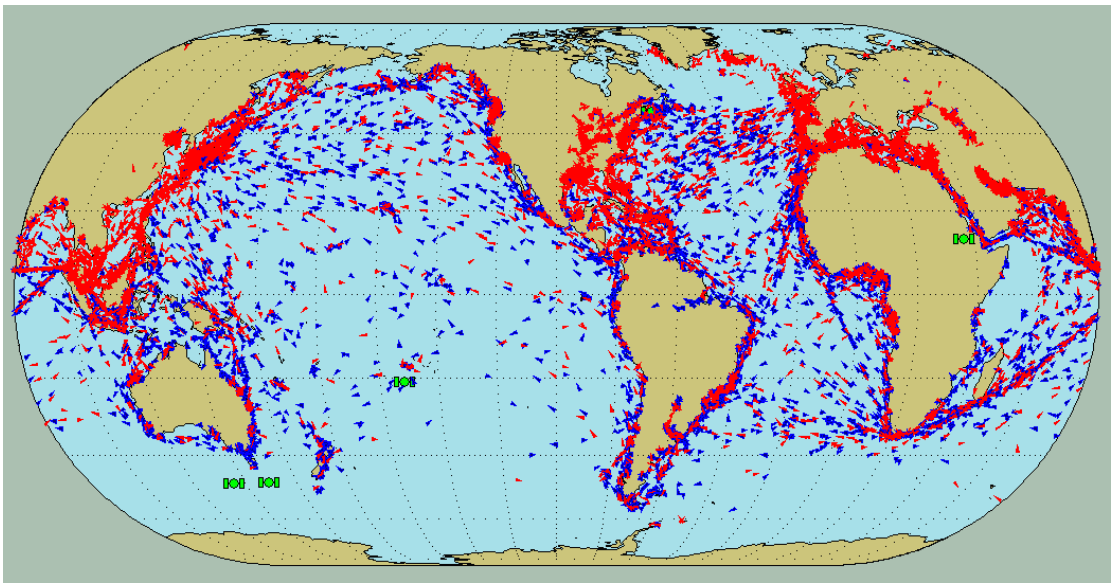

Figure 16. WORLDWIDE AIS TRACKS

Figure 16 is a worldwide AIS plot of over 15,000 contacts, as observed by ORBCOMM satellites over 24 hours. A Norwegian Defense Research Establishment study had analyzed, the ship detection probability for a space-based AIS system with a ship reporting interval of 6 sec, and had calculated that a single satellite at 1000 km altitude will be able to handle up to 900 ships within the field of view with a ship detection probability of better than 99%.

> AIS signals can easily be detected from space by a standard AIS receiver for altitudes up to 1000 km. However, an AIS sensor in space would cover a much larger area on the ground than the AIS system was originally designed for. With many ships within the field of view, interference problems will occur and AIS messages from some of the ships may not be detected. Detailed analyses of the ship detection probability have been performed. Important parameters for the ship detection probability were found to be; the reporting interval ΔT, the observation time *Tobs*, and the number of ships within the field of view. A single satellite at 1000 km altitude (*Tobs*=15 min) would be able to handle up to 900 ships within the field of view with a ship detection probability of better than 99%, with a ship reporting interval of ΔT=6 s.[75]

[75] Høye K. Gudrun, Eriksen Torkild, Meland J. Bente and Narheim T. Bjørn, *Space based AIS for Global Maritime Traffic Monitoring.*

Depending on traffic density, the capability of the AIS-based satellite constellation to handle a larger number of ships can be increased by increasing the number of satellites, lowering the height of the satellite, increasing the reporting interval and / or increasing the observation time. Aerial based AIS is capable of providing ship detection capability of more than 99% at 1000 km, if the number of ships does not exceed its maximum capacity of target handling. Therefore, a constellation of 18 LEO satellites would be able to provide an update of every ship across the globe every 15 minutes, but would still not be able to provide continuous identification capability in time domain for establishing MST. However, if the same LEO satellites are fitted with both SAR and AIS, then these satellites can definitely provide near-real MST.

D. LARGE MARITIME SPACE TRANSPARENCY

Today, the ranges of AIS, which as per design were to operate within 20–40 nautical miles, have been witnessed to extend more than 400 nautical miles into space. A tethered aerostat at 15,000 feet fitted with a sensor suite of radar, AIS, and an electro-optical sensor and IR camera, thus can provide enhanced transparency in maritime space of more than 150 nautical mile radius. As, AIS is capable of providing more than 99% ship detection capability depending on the traffic density 1000 km into space; this system fitted onboard an aerostat at 15,000 feet thus would also provide 99% probability of intercepting ships' transmissions up to its maximum capacity of 4500 ship. As outlined earlier, if there are more than 4500 contacts, those which are further away would automatically be dropped. AIS, along with real-time database of vessels at sea and their precommitted schedule compliance (to prevent spoofing), would provide more than 99% probability of identification of the closest 4500 contacts. Defining a type of radar, such as frequency band, signal processing and various other parameters that contribute towards its probability of detection is not intended to be a part of this thesis; however, to demonstrate the feasibility of

aerostat radars with more than 90% probability of detection against a 5 m2 target at more than 150 miles, particulars of Northrop Grumman's aerostat based-radar AN/TPS-63 (S) are stated below:

> When modified for aerostat use, the TPS-63 radar is reported as being designated as the AN/TPS-63(S) or -63M(S) 'strap modified aerostat' equipment. As an aerostat radar, the sensor is understood to offer a 90 per cent likelihood of detecting a 5 m2 (53.8 sq ft) target (flying at an altitude and range of 150 m (481 ft) and 260 km (161.6 miles) respectively) within a single scan when being operated from an altitude of between 915 m (3,000 ft) and 3,050 m (10,000 ft).[76]

Since aerostats historically have been utilized for detecting low-flying aircrafts and / or missiles, the majority of existing aerostat radars are primarily designed for this role. Nevertheless, these radars can still be utilized for maritime detection, although it would be prudent to fit radar with more than 90% probability of detection against small maritime targets for MST. According to the exhibits and explanations in the previous two chapters, it can be summarized that an aerostat fitted with a sensor suite of radar (90% p (det)) and AIS (99% p (identification)), at 15,000 feet, can provide:

Maritime Space Transparency = p (detection) x p (identification)

(around 150 nautical miles)

= .9 x .99

= 89.1 % for less than 4500 contacts,

if AIS spoofing can be obviated by maintaining a real-time database of vessels at sea, and their compliance to precommitted schedule is ensured.

Additionally, if the aerostats are fitted with electro-optical and IR camera for providing day and night visual identification, the contacts that have been detected but not identified could be classified to further enhance MST. This visual

---

76 "Northrop Grumman AN/TPS-63 (United States), Payloads," *Janes,* http://www.janes.com/articles/Janes-Unmanned-Aerial-Vehicles-and-Targets/Northrop-Grumman-AN-TPS-63-United-States.html (accessed August 26, 2010).

identification capability would also ensure further classification of suspected contacts based on the rules to prevent AIS spoofing.

E. MULTICRITERIA OPTIMIZATION

The number of aerostats required to provide transparency in the desired maritime space would also depend upon the number of targets in the area in addition to the horizon range of aerostats. The number of aerostats, while maintaining Maritime Space Transparency of more than 89%, therefore, would be optimized with Multi-criteria optimization, as this process simultaneously optimizes two or more criteria subject to certain constraints. The process of optimizing the number of aerostats is explained in the succeeding paragraphs.

1. Assumptions

The following have been assumed:

- The targets are randomly distributed in the desired maritime space.
- Both the criteria of horizon range and number of contacts are equally important, as the probability of detection depends upon the former, probability of identification on both, and Maritime Space Transparency is the multiple of both these probabilities.
- Aerostat radar horizon range of 150 nautical miles for an aerostat height of 15,000 feet, the radar horizon range calculation on Page 47 refers.
- All aerostats at same height of 15,000 feet.

2. Decision Variable

Let x = number of aerostat.

3. Optimization

Let r = horizon range of aerostat.
d = desired inter aerostat distance.

e = effective range of aerostat.

c = total coastline.

t = total number of targets.

cc = coastline coverage factor,
(coastline that can be covered by aerostats
/ total coastline).

tc = target coverage factor,
(targets that can be covered by aerostats
/ total number of targets).

a. Desired Inter Aerostat Spacing

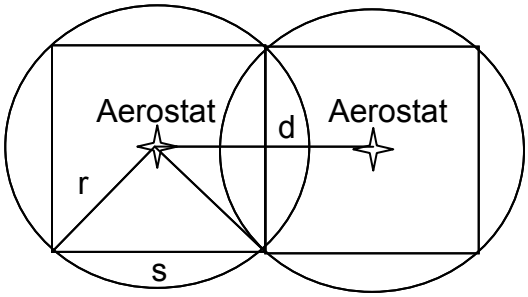

Figure 17. INTER AEROSTAT SPACING

In order to have continuous coverage of area s x 2s, where s is the side of the square within the horizon range (r) of an aerostat, adjacent aerostats would have to be positioned at a distance d (desired inter aerostat distance), as shown in Figure 17.

d = s, from Figure 17

= √ (r^2 + r^2), since the triangle is a right angled

= 2 e

b. Weighted Multiple Criteria Optimization

In mathematical terms, solution of weighted multiple criteria optimization would be written as:

= min (w 1 obj 1 + w 2 obj 2),
x
where obj i is the i-th objective function
w i is the weight of i-th objective function

c. First Objective Function

Objective function y1, minimize x based on horizon range of aerostat

= minimize cc, such that it is atleast 1

= minimize x * e * 2 / c, such that it is = > 1

= minimize x * d / c, such that it is = > 1

= minimize (x * √ (r^2 + r^2)), such that it is = > 1

d. Second Objective Function

Objective function y2, minimize x based on total number of targets

= minimize tc, such that it is at least 1

= minimize x * 4500 / t, such that it is = > 1,
since a single aerostat can receive a
maximum of 4500 targets

e. Optimum Number of Aerostats

The optimum numbers of aerostats, while maintaining Maritime Space Transparency of more than 89%, by weighted multiple criteria optimization would be:

= min (w 1 obj 1 + w 2 obj 2),
x

= min (.5 cc + .5 tc), such that cc and tc are = > 1
x

as both the criteria of horizon range and number of contacts have been assumed to be equally important based on the relationship of probabilities.

The result of the above optimization, based upon the length of the coastline and maximum number of targets along this coastline by utilizing the solver function of excel, is tabulated and graphed in Table 4 and Figure 18, respectively.

Coast Line	No of targets	No of aerostats	RHR	Inter aerostat dist	Obj fun 1	Obj fun 2	MCO
(nm)		x	r	d			
200	4500	1	150	212.13	1.06	1.00	1.03
300	4500	2	150	212.13	1.41	2.00	1.71
400	4500	2	150	212.13	1.06	2.00	1.53
500	4500	3	150	212.13	1.27	3.00	2.14
400	9000	2	150	212.13	1.06	1.00	1.03
500	9000	3	150	212.13	1.27	1.50	1.39
600	9000	3	150	212.13	1.06	1.50	1.28
700	9000	4	150	212.13	1.21	2.00	1.61
700	13500	4	150	212.13	1.21	1.33	1.27
800	13500	4	150	212.13	1.06	1.33	1.20
900	13500	5	150	212.13	1.18	1.67	1.42
1000	13500	5	150	212.13	1.06	1.67	1.36

Table 4. OPTIMUM NUMBER OF AEROSTATS TABLE

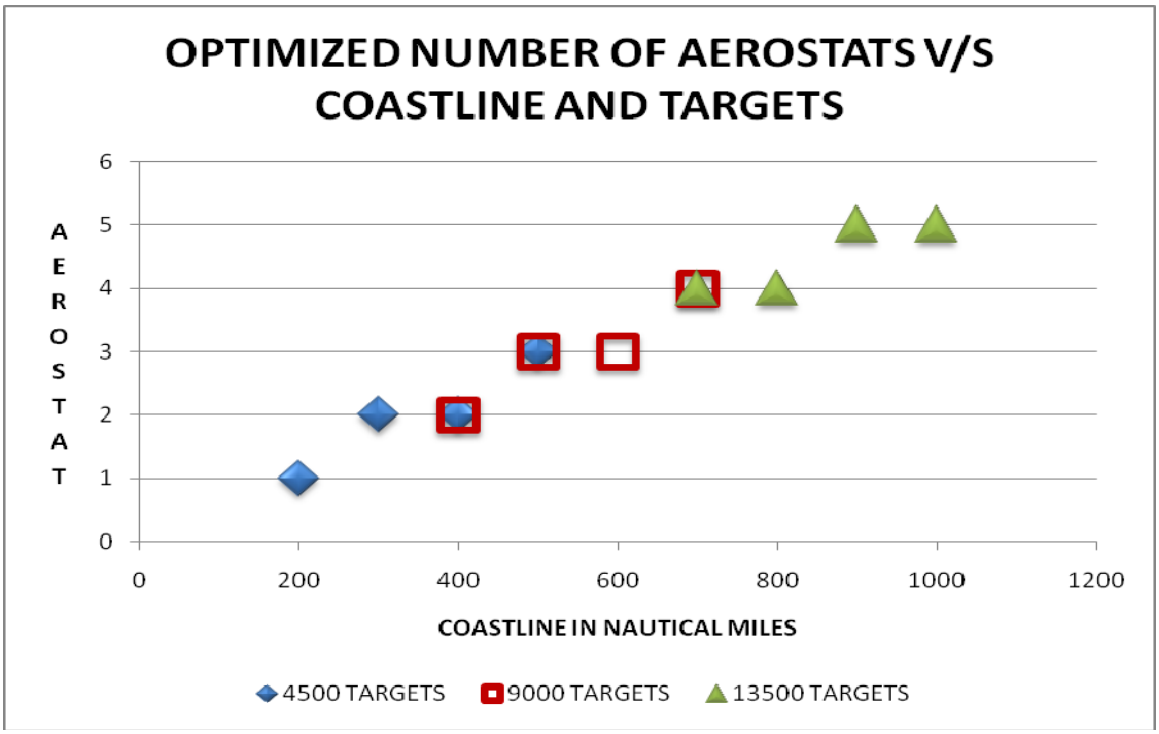

Figure 18. OPTIMUM NUMBER OF AEROSTATS GRAPH

As can be observed from Table 4 and Sub-para D of this chapter, three aerostats with appropriate sensors suite of radar (90% p (det)) and AIS (99% p (identification)), at 15,000 feet, can provide more than 89% MST along a coastline of up to 600 nautical miles for a maximum of 9000 AIS targets, by obviating AIS spoofing. This capability of the coastal surveillance system could be assumed to be an absolute payoff of value 8 for the terror victim state in the Game Theory setup of Chapter II. An absolute payoff of 8 has been assumed for the terror victim state based on 89% MST from the existing technologies because in the near future there could be more promising technologies that could further enhance the capability of maritime surveillance in territorial sea, thereby increasing this payoff to its maximum value of 9. Revisiting the analysis of the Game Theory in Chapter II, indicates that the security level of (5,2) without an effective coastal surveillance, could be increased to (8,2) by the terror victim state by enhancing its coastal surveillance against small boats utilizing optimum number of aerostats with an appropriate sensor suite. Though this still would not

be a Pareto optimum solution, it would place the terror victim state in a much more advantageous position to coerce the terror origin state to take action against the terrorist organizations operating from its territory. Even if the terror origin state does not act against the terrorist organizations, a security level payoff of 8 for the terror victim state achieved by enhancing coastal surveillance against small boats, would provide an excellent strategy against the small boat terror attacks in territorial sea.

V. WAY AHEAD

A. CONCLUSION

In today's information age, where information travels faster than a bullet: small boat terrorism in territorial sea has been transnationalized and revolutionized by the terrorists by exploiting commercially-available-off-the-shelf-technologies like GPS, smart phones, satellite maps/charts/picture and Internet application like social networking, etc. It is now the turn of the counterterrorism security forces to utilize the speed of information to counter the bullets and bombs of these terrorists. Tomorrow, there could still be more voices articulating better ways to counter the threat of small boat terrorism in territorial sea, but the strategy recommended by this thesis is akin to what Sun Tzu opined, "know your enemy and know yourself and you can fight a hundred battles without disaster."[77] Although countering maritime terrorism by eliminating terrorists on land is unquestionably the better solution, as analyzed by Game theory the payoffs for offensive action against terrorists' base camps in another country would be very high financially and in terms of human resources. The preferred option for the country as per this analysis should be to utilize its MDA in the territorial sea to counter the threat of small boat terrorism in these waters. According to a historic analysis of maritime terrorism in Israel, analysis of Israeli coastal defense, corroboratory evidence of Singapore harbor, and analysis of existing technologies, it can be summarized that attaching a network of optimum number of aerostats fitted with a sensor suite of radar, AIS, and electro-optical sensor, together with the existing MDA, can provide enhanced transparency in large maritime space to counter threat of small boat terrorism in territorial waters. It is necessary, however, that the existing policy of AIS be amended to role based fitment and that the spoofing of these systems is obviated by maintaining a real-time database of vessels at sea and ensuring their compliance to precommitted schedule. Additionally, the inputs of SAR and AIS from a constellation of LEO

[77] Sun Tzu, "The Art of War."

satellites could be utilized to augment the existing MDA, which would also assist in further enhancing the MST in the territorial sea. Concluding the thesis with Yarger's strategy model, which says "strategy is all about how (way or concept) leadership will use the power (means or resources) available to the state to exercise control over sets of circumstances and geographic locations to achieve objectives (ends)"[78], MDA can be adapted to the territorial sea, by incorporating a network of relevant sensors to enhance MST in order to reduce the information asymmetry between terrorists and maritime security forces, which would in turn provide actionable intelligence in the form of a Common Operating Picture (COP) to interdict small boat heading for terror attacks in these waters.

B. RECOMMENDATIONS

It is undoubtedly true that the information age today has linked the terrorists across the continents, and thus to avoid the possibility of small boat terror attacks, similar to the 2008 Mumbai terror attacks, in future and against other countries, especially those combating terrorism, the following are recommended:

- **Role based AIS fitment policy**. The present AIS fitment policy, which is based on the size of the vessel (above 300 tons) in accordance with International Maritime Organization,[79] should be amended to a role-based policy, mandating the fitment of this equipment on vessels proceeding outside the contiguous zone or territorial sea (in the absence of contiguous zone) into the International Waters, irrespective of the size of the vessel.
- **Identification Zone**. Promulgation of an identification zone of 40 – 80 nautical miles outside the contiguous zone, catering for an intercept capability of 2 – 4 hours against a 20 knots target, in

78 Harry R. Yarger, "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model."

79 *IMO adopts comprehensive maritime security measures,* December 13, 2002.

which enhanced MST is maintained continuously in both time and spatial domain, in order to identify the suspected targets. Countries sharing the limit of their territorial waters could mutually work out the size of the identification zone either side of this limit based on their enforcement capability.

- **Real-time database of friendly contacts at sea**. Maintenance of real-time data base of all friendly contacts at sea with self login capability based on security token (like, smart card), pass phrase (like, password based encryption key) and geographic location (like, GPS based position) based multi-factor authentication should be ensured to obviate AIS spoofing.
- **Compliance with precommitted schedule policy**. Ensure the compliance of all vessels transiting in and out of the contiguous zone or territorial sea (in the absence of contiguous zone), to a precommitted schedule in order to identify suspected targets.
- **Emergency alarm function**. Incorporation of an emergency alarm button in the AIS to provide immediate threat warning of incidents such as hijacking. This feature would also function as an early warning system from a fleet of friendly vessels operating in the International Waters outside the contiguous zone.
- **Aerostat based network of sensors**. A network of an optimum number of aerostat fitted with a sensor suite of radar, AIS, and electro-optical and IR camera, should be amalgamated with the existing MDA to enhance MST
- **Space-based AIS**. Orbcomm constellation of 18 VHF data capable LEO satellites, once operational in 2012, should be utilized to augment the worldwide MDA, as it would provide global AIS update of vessels every 15 minutes. Despite the fact that the present

update rate of AIS capable LEO satellites is far from desired, but their output still can be utilized for enhancing the existing MDA.

- **LEO satellites for detection and identification**. While a constellation of LEO satellites fitted with SAR and AIS may not be able to provide continuous detection and identification capability in the time and spatial domains, but if this all weather global capability can be made near-continuous a constellation of such satellites along with other platforms could be utilized for enhancing the MST.

LIST OF REFERENCES

"1974 Islamic Terrorism Timeline." *Prophet of Doom .* November 16, 2006. http://www.prophetofdoom.net/Islamic_Terrorism_Timeline_1974.Islam (accessed June 21, 2010).

Barnett, Thomas P. M. *Great Powers: America and the World After Bush.* New York: Penguin Group, 2009.

Belasco, Amy. *The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11.* CRS Report for Congress, Congressional Research Service, 2009.

Bole, Alan, Dineley, Bill and Wall, Alan. *Radar and ARPA.* Burlington: Oxford, 2005.

Bolkcom, Christopher. *Potential Military Use of Airships and Aerostat.* CRS Report for Congress, CRS Web, 2005.

CNN Transcripts. July 28, 2006. http://transcripts.cnn.com/TRANSCRIPTS/0607/28/sitroom.02.html (accessed June 21, 2010).

Consortium for Mathematics. *For All Practical Purposes: Introduction to Contemporary Mathematics.* New York: W H Freeman & Company, 1996.

Daly, John C. K. "Terrorism and Piracy: The Dual Threat to Maritime Shipping." *Global Terrorism Analysis.* August 15, 2008. http://www.jamestown.org/programs/gta/Terrorism and Piracy The Dual Threat to Maritime Shipping - The Jamestown Foundation.mht (accessed February 07, 2010).

"DHS' Strategy and Plans to Counter Small Vessel." *Department of Homeland SecurityOffice of Inspector General.* September 2009. http://www.dhs.gov/xoig/assets/mgmtrpts/OIG_09-100_Sep09.pdf (accessed March 02, 2010).

Dziewicki, Marek. *The Role of AIS for Small Ships.* Department of ATON Technique and Radionavigation Systems Report, Gdynia. BalticMaster Gdynia, February 2007.

Geneva Academy of International Humanitarian Law and Human Rights. http://www.adh-geneva.ch/RULAC/qualification_of_armed_conflict.php (accessed May 07, 2010).

Godfrey, Mike. *U.S. Boat Association Reproaches Small Boat Tracking Proposals.* December 16, 2009. http://www.tax-news.com/asp/story/story_marine.asp?storyname=40704 (accessed March 02, 2010).

Goswami, Namrata. "IDSA Comment - Mumbai Attacks: A Deadly Performance." *Institute of Defence Studies & Analysis.* December 05, 2008. http://www.idsa.in/idsastrategiccomments/MumbaiAttacks_NGoswami_051208 (accessed January 26, 2010).

Goward, Dana. "Maritime Domain Awareness — The Whole is Greater than the Sum of its." *U.S. Coast Guard.* April 20, 2009. http://www.uscg.mil/comdt/blog/2009/04/maritime-domain-awareness-whole-is.asp (accessed March 02, 2010).

Gudrun Høye K., Torkild, Eriksen, Bente, Meland J. and Bjørn, Narheim T. *Space based AIS for Global Maritime Traffic Monitoring.* Norway: Norwegian Defence Research Establishment, 2007.

IAI ELTA System Ltd. http://www.iai.co.il/sip_storage/files/2/36842.pdf (accessed July 01, 2010).

IMO adopts comprehensive maritime security measures. December 13, 2002. http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689 (accessed January 22, 2010).

Ince Nejat, Topuz, Ercan, Panayirci Erdal and Isik Cevdet. *Principles of Integrated Maritime surveillance System.* Norwell: Kulwer Academic Publisher, 1999.

Lorenz, Akiva J. "The Threat of Maritime Terrorism to Israel." *International Institute for Counterterrorism.* September 24, 2007. http://www.ict.org.il/Articles/tabid/66/Articlsid/251/currentpage/6/Default.aspx (accessed February 14, 2010).

"Maritime Domain Awareness." *GlobalSecurity.org.* http://www.globalsecurity.org/intell/systems/mda.htm (accessed May 07, 2010).

McCormick, Gordon H. *Defence Analysis Class.* Naval Postgraduate School, Monterey. July 16, 2009.

"Northrop Grumman AN/TPS-63 (United States), Payloads." *Janes.* http://www.janes.com/articles/Janes-Unmanned-Aerial-Vehicles-and-Targets/Northrop-Grumman-AN-TPS-63-United-States.html (accessed August 26, 2010).

Palestine Facts: What was the Litani River Operation, Israel's invasion of Lebanon in 1978? http://www.palestinefacts.org/pf_1967to1991_lebanon_1978.php (accessed June 21, 2010).

Presse, Agence France. "Singapore beefs up maritime security, installs transponders on small vessels." *Singapore Windows.* July 01, 2005. http://www.singapore-window.org/sw05/050701a1.htm (accessed July 01, 2010).

"RADARSAT-2." *Imaging Notes.* Fall 2008. http://www.imagingnotes.com/go/article_free.php?mp_id=147 (accessed August 24, 2010).

"RCM (RADARSAT Constellation Mission)." *eoPortal.* http://www.eoportal.org/directory/pres_RCMRADARSATConstellationMission.html (accessed August 24, 2010).

Rusling, Matthew. "No Silver Bullet for Thwarting Terrorists Aboard Small Boats." *National Defense Industrial Association.* March 2009. http://www.nationaldefensemagazine.org/archive/2009/March/Pages/NoSilverBulletforThwartingTerroristsAboardSmallBoats.aspx (accessed June 30, 2010).

Samarasinghe, Vice Admiral Thisra. "Sri Lankan Navy's role in eradicating international maritime terrorism." *Sri Lanka Guardian.* October 25, 2009. http://www.srilankaguardian.org/2009/10/sri-lankan-navys-role-in-eradicating.html (accessed May 07, 2010).

"Satellite-Based AIS: One Giant Leap for Vessel Tracking." *Boats.* June 06, 2010. http://features.boats.com/boat-content/2010/06/satellite-based-ais-one-giant-leap-for-vessel-tracking/ (accessed August 24, 2010).

"Security Council Resolutions - 1978." *United Nations.* http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/368/71/IMG/NR036871.pdf?OpenElement (accessed June 24, 2010).

State of Israel Ministry of Transport and Shipping. http://en.mot.gov.il/index.php?option=com_content&view=article&id=145:rad17m&catid=17:noticetomariners&Itemid=12 (accessed January 30, 2010).

"Statement in the Knesset by Defence Minister Peres." *Israel Ministry of Foreign Affairs.* March 11, 1975. http://www.mfa.gov.il/MFA/Foreign%20Relations/Israels%20Foreign%20Relations%20since%201947/1974-1977/68%20Statement%20in%20the%20Knesset%20by%20Defence%20Minister%20Pe (accessed June 21, 2010).

Straffin, Philip D. *Game Theory and Strategy.* The Mathematical Association of America, 1975.

Trager, Robert F. and Zagorcheva, Dessislava P. "Deterring Terrorism: It Can be Done." *International Security 3, no. 3*, Winter 2005/06.

Tzu, Sun. "The Art of War ." *Classics Archive.* http://classics.mit.edu/Tzu/artwar.html (accessed April 21, 2010).

"United Nations Convention on the Law of the Sea - Part II." *United Nations web sites.* http://www.un.org/Depts/los/convention_agreements/texts/unclos/part2.htm (accessed March 01, 2010).

U.S. Air Combat Command. http://www.acc.af.mil/library/factsheets/factsheet.asp?id=2359 (accessed July 07, 2010).

U.S. Department of Homeland Security - AIS. http://www.navcen.uscg.gov/?pageName=AIS (accessed July 01, 2010).

"U.S. National Plan to achieve Maritime Domain Awareness." October 2005. http://www.virginia.edu/colp/pdf/NSMS-National-Plan-to-Achieve-Maritime-Domain-Awareness.pdf (accessed March 02, 2010).

U.S. National Strategy for Combating Terrorism. https://www.cia.gov/news-information/cia-the-war-on-terrorism/Counter_Terrorism_Strategy.pdf.

U.S. Nationwide Automatic Identification System (NAIS). http://www.uscg.mil/ACQUISITION/nais/ (accessed March 02, 2010).

"The USA's RAID Program: Small Systems, Big Surveillance Time." *Defense Industry Daily.* July 19, 2009. http://www.defenseindustrydaily.com/the-usas-raid-program-small-aerostats-big-surveillance-time-02779/ (accessed February 07, 2010).

Yarger, Harry R. "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model." In *USAWC Guide to National Security Issues, Vol I: Theory of War and Strategy*, 43-49. Carlisle, United States: Strategic Studies Institute of the U.S. Army War College (SSI), 2008.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Integrated Headquarters of
   Ministry of Defense (Navy)
   New Delhi, India